NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A NETWORK DESIGN APPROACH TO COUNTERING TERRORISM

by

Linus P. Torner

September 2015

Thesis Advisor: Sean F. Everton
Second Reader: Steven J. Iatrou

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE A NETWORK DESIGN APPROACH TO COUNTERING TERRORISM			**5. FUNDING NUMBERS**
6. AUTHOR(S) Torner, Linus P.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Several recent terrorist attacks in Western countries have highlighted the need for strategies to disrupt dark networks, and social network analysis (SNA) has proven to be a useful tool for analyzing network structure and identifying weaknesses, based on empirical data. But there are several other factors to consider, and by taking a network design approach, a better understanding can be gained of how networks function and what makes them successful. This thesis applies a conceptual network design approach, together with SNA, in a comparative case study where performance of historical terrorist networks is examined to find recommendations for future counter-terrorism efforts. The conclusion is that design matters; results depend on how well networks are configured for the specific environment, and the network design approach can be used together with SNA to identify vulnerabilities for exploitation. Networks require a balanced configuration to perform well; studying several endogenous and exogenous factors can help counter-terrorism services remove that balance for terrorist networks, and design their own networks to be as efficient as possible. To be successful, counter-terrorist organizations must out-design the terrorist networks.

14. SUBJECT TERMS terrorism, social network analysis, information operations, network warfare			**15. NUMBER OF PAGES** 119
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A NETWORK DESIGN APPROACH TO COUNTERING TERRORISM

Linus P. Torner
Captain, Swedish Army
M.S., Chalmers University of Technology, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2015

Approved by: Dr. Sean F. Everton
Thesis Advisor

Steven J. Iatrou
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Several recent terrorist attacks in Western countries have highlighted the need for strategies to disrupt dark networks, and social network analysis (SNA) has proven to be a useful tool for analyzing network structure and identifying weaknesses, based on empirical data. But there are several other factors to consider, and by taking a network design approach, a better understanding can be gained of how networks function and what makes them successful. This thesis applies a conceptual network design approach, together with SNA, in a comparative case study where performance of historical terrorist networks is examined to find recommendations for future counter-terrorism efforts. The conclusion is that design matters; results depend on how well networks are configured for the specific environment, and the network design approach can be used together with SNA to identify vulnerabilities for exploitation. Networks require a balanced configuration to perform well; studying several endogenous and exogenous factors can help counter-terrorism services remove that balance for terrorist networks, and design their own networks to be as efficient as possible. To be successful, counter-terrorist organizations must out-design the terrorist networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

During my time at NPS in Monterey, I was lucky to meet a lot of inspiring people. Both students and faculty showed a high degree of knowledge and motivation. This led to many interesting discussions where experiences from various contexts and countries were shared.

There are a few persons that I would like to notice. First, I want to thank Dr. Sean F. Everton for working with me on this thesis, and for introducing me to the concepts of social network analysis and dark networks. Next, I would like to thank Dr. Nancy Roberts for enlightening me about network design, and for many stimulating discussions. Also, I am grateful for the support and guidance of Mr. Steven J. Iatrou throughout my studies at NPS.

Finally, I would like to thank the Swedish Armed Forces and my superiors for letting me go to Monterey to get an incredible experience and a lot of new knowledge.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Global war on terrorism is escalating as ISIS[1] has taken a place beside al-Qaeda with intention, capacity, and opportunity to strike in Western countries; therefore, fear of attacks is increasing in both the United States and in Europe. Recent events have proved that the terrorist threat is real, and there is a high probability that there are sleeper terrorist cells waiting to strike against citizens of any country that is supporting the war on terrorism. To counter this threat, law enforcement agencies must be able to identify and disrupt such cells before they can achieve their objectives. But to craft efficient strategies to disrupt terrorist cells, an understanding of how they function is required. So how are terrorist networks analyzed? Social network analysis (SNA) offers one relational approach to analyze networks and find ways to disrupt them. Here an additional approach is suggested; network design analysis, which aims to understand how the cells are designed. This thesis examines what explanatory value the two different models have and how they can be used together. If the models have merit, they can be applied in the pursuit of strategies to disrupt terrorist networks. What insights the two models provide about how terrorist networks function are discovered by applying both models to historical cases, and from those insights strategies can be crafted to disrupt present and future terrorist cells. The goal of this study is to improve means to craft strategies and policies for disrupting terrorist networks by exploring an alternative analysis perspective.

A. OVERVIEW OF THE SUBJECT

The threat of terrorist attacks has probably risen with the increasing engagement against ISIS, which recent events in France and Belgium support.[2] There is a concern across Europe about jihadist fighters that return from conflict zones. Using their

[1] The Islamic State of Iraq and Syria (ISIS) is used here to refer to the Islamic extremist group trying to establish an Islamic caliphate in Iraq and Syria. Other common names for the same group are The Islamic State of Iraq and the Levant (ISIL), or just Islamic State (IS).

[2] Al-Qaeda followers attacked the Paris office of French satirical newspaper *Charlie Hebdo* on January 7, 2015. Two days later, an ISIS follower attacked a market in Porte de Vincennes, France. On January 15, 2015, Belgian police raided a terrorist cell in Verviers where the terrorists had ties to ISIS in Syria. These events are described more thoroughly in Chapter II.

experience they may set up terrorist cells that support or conduct terrorism related activities.

Governments battle this threat by developing strategies and policies to disrupt terrorist networks. The strategies are based on an understanding of the networks: how they function and what their weaknesses are. SNA is one popular analysis model where various relations between actors in a network are mapped, and there is extensive work published of SNA of different illegal or covert networks. This relational approach may identify weaknesses in the network that can be exploited. One method is to find central actors in the network and then try to remove them. Another tactic is to identify structural holes in a network where informants can be inserted. Despite the benefits from SNA, there are still limitations. SNA is a collection of theories and methods for empirically measuring a network's structure. It can identify strengths and weaknesses in a network, but an understanding of what makes a network successful in a particular environment is also valuable. Structure is only one aspect of a network; there are several other endogenous and exogenous factors that affect network performance.

Network design is a method that can complement SNA in understanding terrorist networks. It considers the internal design of a network and evaluates how well the network is configured for a specific environment. Terrorist cells are systems operating in an environment with purpose, direction, and different internal processes such as communication, planning, human resources, and financing. A greater understanding of the networks may be gained by considering how all these parts are configured.

B. PURPOSE AND SCOPE

The Western world has experienced several devastating terrorist attacks, and there is little doubt that more will occur. The war on terrorism is a global campaign, but attention is also needed on local elements already preparing attacks. Even though the larger picture is important—to combat leadership, recruitment, and propaganda—methods to disrupt sleeper terrorist cells are needed to prevent imminent attacks. The scope of this thesis is to examine and discuss local terrorist cells ready to strike, not global terrorist networks as a whole. Even though the unit of analysis here is small

terrorist cells that are conducting the attacks, the analysis models can be applied to networks of various sizes.

The purpose of this thesis is to examine a network design model as an additional approach for developing strategies to disrupt sleeper terrorist cells before they can execute their plans. These strategies are supposed to be a contribution to the strategies available for preventing terrorist attacks. The research shows that this additional model is applicable in answering several key questions. Is there something in the internal design of terrorist cells that makes them successful? If so, it may be something that can be exploited. Does the network design approach have merit, and does it provide explanatory value of how to take down terrorist cells? What added value does the network design model provide?

By using a network design approach together with SNA, new strategies to disrupt terrorist cells may be identified. The network design approach is not supposed to replace SNA; it offers a complementary perspective. Key design factors that make a terrorist cell successful or not are incorporated into suggested strategies and policies. The strategies aim to disrupt generic sleeping terrorist cells in Western countries.

The study is limited to the information that is publically available on previous terrorist attacks. All sources are strictly unclassified. It is possible that more accurate conclusions may be drawn with access to classified information, but that is not within the scope of this thesis.

C. METHOD

First, a literature review is conducted about the terrorist threat, network theory, and methods to disrupt dark networks to learn what other studies have found in these areas. Findings are incorporated into the development of a research design that includes a framework to apply SNA and network design to the analysis of previous cases of terrorist attacks.

Both analysis models are applied to two historical cases to determine how they offer explanatory value and how they can contribute to a better understanding of terrorist

cells. Using the models to analyze historical cases shows how each approach can provide insight into the internals of a network. Both approaches are valid, but they provide different information. A combination of the two is suggested to provide a more complete picture. SNA can be used to identify weaknesses and targets in a network from empirical data, and the network design approach can determine what structure is more efficient in a particular environment. By taking a network design approach, what really is going on internally in networks can be showed, and by understanding the internal dynamics of terrorist networks, they can be disrupted more effectively. Network design considers a larger set of factors than SNA, and looks at how they are pieced together to produce results in a specific environment.

A framework is used to describe and analyze the cases from a network design perspective. This is a descriptive model, which presents a conceptual map of a network. It has not been proved, but this thesis demonstrates how it can be applied to describing terrorist networks with the intent to intervene.

Based on insights from using the two models together, generic strategies to disrupt terrorist cells are proposed. By learning from previous events, future terrorist attacks may be prevented.

II. ANALYSIS OF TERRORIST NETWORKS

As Sun Tzu remarked in *The Art of War*, you are more likely to defeat your adversary if you know him well. This chapter reviews the current terrorist threat. The concept of terrorist networks is broken down into its components, terrorism and networks. Both parts are examined and defined based on previous research. First, terrorism is discussed, including descriptions of threats, motives, methods, and recent events. Current problems and issues are also highlighted. Next, network theory is introduced, with basic definitions and concepts. Through the study of network theory, a framework for analysis is defined. This framework is then used to design the model of analysis.

A. THE TERRORIST THREAT

In 2004, Sageman examined a social movement that he calls the Global Salafi jihad, defined as terror groups that want to establish an Islamic state by defeating Western powers. The movement includes several different groups, al-Qaeda being the vanguard (Sageman, 2004, p. 1). Referencing 172 biographies of terrorists, he examined a "new type of terrorism, driven by networks of fanatics determined to inflict maximum civilian and economic damage on distant targets in pursuit of their extremist goals" (Sageman, 2004, p. vii). His investigation suggested that "this form of terrorism is an emergent quality of the social networks formed by alienated young men who become transformed into fanatics yearning for martyrdom and eager to kill" (Sageman, 2004, p. vii). Although an important question, it is beyond the scope of this thesis to explain the social and situational circumstances that make people join terrorist organizations. Instead, the focus here lies on the terrorists who are ready to strike, regardless of what path led them there. So what threats are out there?

In the beginning of the 21st century, al-Qaeda was considered the largest threat. Following 9/11, the war on terrorism was essentially equated to war against al-Qaeda. The hunt for Osama bin Laden has been the most prioritized task for U.S. intelligence agencies, an undertaking that President Obama even campaigned on. As he stated in the

presidential debate on October 7, 2008, “We will kill bin Laden. We will crush al-Qaeda. That has to be our biggest national security priority” (The Commission on Presidential Debates, 2008). This shows how much focus was put on al-Qaeda at the time.

Many salient terrorist attacks on American or European soil in the early 2000s have either been claimed by or attributed to al-Qaeda.[3] But recently ISIS has taken its place as an adversary beside al-Qaeda. With the war against ISIS increasing, the threat of terrorist attacks arranged by ISIS has, and probably will, increase. When air strikes against ISIS commenced, ISIS changed its focus and ordered attacks in Europe. Earlier, the priority had been to establish an Islamic caliphate (Cruickshank, Castillo, & Shoichet, 2015). Methods and motivation are similar between the organizations, and the result can be devastating regardless of the perpetrator. What organizations terrorists ally with is not considered in this thesis. Instead, similarities between historical terrorist attacks are discussed and generic policies and strategies are proposed. Some common characteristics of terrorist networks are described next.

1. Motives

Terrorist organizations generally want to cause maximum civilian and economic damage to their targets (Sageman, 2004). Sometimes they have a specific goal in mind, as in Madrid in 2004 where the attacks led to Spain withdrawing their troops from Iraq (Rodriguez, 2005). In other cases, the goal is to inflict as much damage as possible to the enemy to reduce their will to fight. Often terrorists seek extensive media coverage with the intent to demoralize the domestic population and reduce public support for the war on terrorism. Terrorists seek to achieve their objectives through carefully planned attacks that will attract media attention and are against targets chosen for high publicity and their ability to influence the intended audience (Emery, Earl, & Buettner, 2004).

In the book about his work in Afghanistan and Pakistan, Mortenson (2007) argues that the United States created many terrorists with their 2001 attack on Afghanistan. There is a saying that killing one terrorist creates 10 more, referring to relatives and

[3] Examples of attacks include 9/11, Riyadh suicide bombings in 2003, Istanbul bombings 2003, Madrid train bombings in 2004, and London public transport bombings in 2005.

friends who want to take revenge on the actor responsible for their loved one's death. Many victims of bombings in Afghanistan, Iraq, and Syria consider the United States, and its allies, enemies that must be fought at all costs. Terrorist organizations focus on these victims when recruiting new members.

2. Organization and Methods

Terrorist cells vary in size and shape, but some characteristics are similar between them. They are examples of *dark networks*, a term for a covert and illegal network that tries to conceal itself and its activities from authorities (Everton, 2012; Milward & Raab, 2006).

The methods terrorists use to reach their goals can vary depending on available resources, the nature of the target, the environment, and time available to prepare. Historical examples show that terrorists target areas with many potential victims. Public transportation systems have been targeted in London and Madrid, and central parts of large cities are popular targets, especially if there is an event going on like at the Boston Marathon in April 2013. In all these cases, remote detonated bombs were utilized. The 9/11 attacks were one of a kind: Never before has such a complex attack been performed. That level of complexity is rare; it requires a lot of preparation and resources. But it had a great effect, at least in the short run. Besides killing thousands of people, Osama bin Laden wanted to send a message around the world that would influence both adversaries and allies (Emery et al., 2004). Bin Laden and his supporters expected that the attacks would deter governments from supporting the global war on terrorism while increasing morale among extremists by showing that even the United States is vulnerable. This was an example of terrorist information operations, where information "induces fear in one audience, while at the same time elicits sympathy and support from others" (Emery et al., 2004, p. 35). Perhaps Osama bin Laden did not foresee the forceful response of the United States that led to the fall of the Taliban and eventually his own death. Instead of being broken down by the attack, the country united and became more determined than ever to fight terrorism.

Terrorist cells share some properties, for example, the need for training, coordination, and resources. They need personnel that can move freely enough to get close to the target. This is easier if the terrorist organization is able to recruit citizens of the country where the attack is planned. Money and supplies are other required resources, together with some kind of munitions, whether it is guns, bombs, or chemical or biological agents. The terrorists have to be trained to use these munitions, and the better trained they are the more likely the attack is successful. Not only do they have to learn how to handle weapons, but they also must learn how to blend in to the operational environment and to avoid raising suspicion. To remain undetected, terrorists must be cautious of how they use communications, credit cards, transportation, and other elements that leave traces.

3. Recent Events

Early in 2015, France experienced a series of events that put Paris next to London and Madrid on the list of European capitals that have suffered major terrorist attacks. The satirical magazine *Charlie Hebdo* was attacked on January 7 by two gunmen who stormed their Paris office and killed 12 people (Astier, 2015). The magazine had upset Muslims around the world by publishing cartoons of the Prophet Muhammad. Police killed the two brothers suspected of the massacre two days later. That same day another perpetrator took several people hostage in a Jewish supermarket in eastern Paris and killed four more people (Astier, 2015). The perpetrators are all believed to be members of the same Islamic group in Paris with ties to al-Qaeda ("Paris Attacks," 2015; Sage, 2015).

Just one week after the attacks in Paris, Belgian counter-terrorism agencies conducted a series of raids against a network with connections to ISIS (Cruickshank et al., 2015). The most prominent raid took place in Verviers on January 15 where two suspects were killed and one was captured. The police found large amounts of guns, munitions, and explosives during the raids. They also confiscated police uniforms and a large amount of money. Authorities believe that the terrorists were planning to kill police officers ("Belgium Deploys," 2015).

After Italian police discovered indications of preparations of a possible attack, they made nine arrests on April 24, 2015. The extremists had ties to al-Qaeda and might have planned a bomb attack against the Vatican in 2010 according to investigators ("Italy Investigators," 2015). Police said the suspects came from Afghanistan and Pakistan and accused them of staging attacks against the Pakistani government. Two of the men are reported to have been bodyguards to Osama bin Laden (Povoledo, 2015).

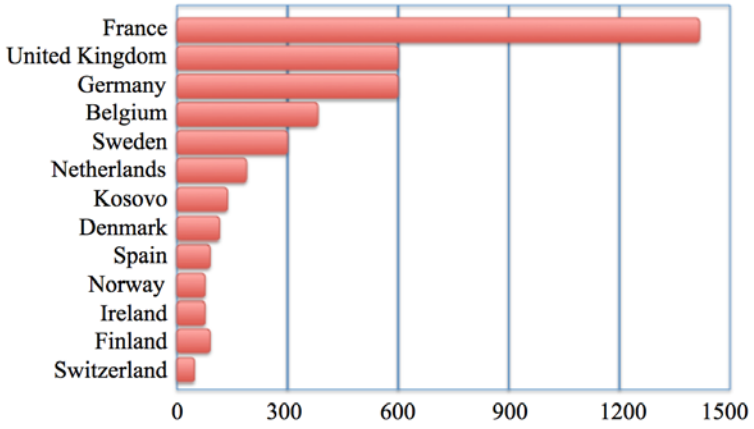
These recent examples show that the threat of terrorist attacks is clear and present. Evidently there are terrorist cells out there preparing to strike. Thankfully, some are caught before they can carry out an attack. But more tools are needed to detect and disrupt these terrorist cells. In the next section, a big concern in Europe is discussed: ISIS fighters returning from Syria and Iraq.

4. Current Issues

Citizens who return to their home countries after participating in terrorist activity in war zones such as Syria and Iraq are one of the biggest concerns in Europe currently. As the European law enforcement agency Europol stated in its 2014 European Union terrorism situation and trend report, "There is a growing threat from EU citizens, who, having travelled to conflict zones to engage in terrorist activity, return to the European Union with a willingness to commit acts of terrorism" (Europol, 2014).

It is unclear how many Europeans have joined ISIS in the last couple of years; some speculate that it is more than 3,000 individuals (Cruickshank et al., 2015). In several cases, returning ISIS fighters have been connected to attack plans in Europe (Cruickshank et al., 2015). One example is the recent anti-terror operation in Belgium described earlier, which targeted a group of returnees (Cruickshank et al., 2015). According to CNN, "the ongoing terror threat appears to involve up to 20 sleeper cells of between 120 to 180 people ready to strike in France, Germany, Belgium and the Netherlands" (Cruickshank et al., 2015). Fighters have travelled from many different countries to participate in violent extremism. Figure 1 presents an estimate by BBC from 2013 of the nationalities among the foreign fighters.

Figure 1. Foreign Fighters from Europe Involved in Iraq and Syria.



(After "Belgium Deploys Troops," 2015)

The Swedish Security Service (2015) believes that al-Qaeda–inspired persons and groups exerting violent Islamism constitute the largest terrorist threat against Sweden. Some of the threats identified during the last three years have involved persons who have returned to Sweden after participating in violence abroad (Swedish Security Service, 2015). Both men and women travel abroad to join violent Islamic groups. Most men are between 18 and 30 years old and actively participate in fights, while women often marry men who fight, or support the groups logistically (Swedish Security Service, 2015). Motives vary, but often it is considered a religious duty to support these groups (Swedish Security Service, 2015). At the time of this thesis, it is not illegal for persons in Sweden to travel to join these groups, but by participating in violent activities, they can be guilty of war crimes or terrorism. This makes it hard to prevent people from leaving and creates a threat when they return to Sweden. Returning fighters have been exposed to radical ideologies and have become more likely to perform terrorist attacks (Swedish Security Service, 2015). They may recruit and convince more people to leave, or create terrorist cells in their home countries. Authorities fear that they can plan terrorist attacks or support terrorist activities financially, logistically, or in other ways. There is a common European concern about returnees since many European citizens can travel easily between different European countries. Therefore, European countries have a shared responsibility to cooperate against this threat (Swedish Security Service, 2015). Some

returnees are expected to pose a more serious threat than others. Between the different groups that EU citizens fight in, "those fighting alongside al-Qaeda-affiliated groups, such as the ISIL and Jabhat al-Nusra, were believed to amount to a significant number and, ultimately, pose the greatest threat to the EU" (Europol, 2014, p. 12).

Concerned European countries have adopted different approaches to deal with returning fighters. Some make it illegal to travel abroad to join violent Islamic groups, and returnees are faced with charges of war crimes, terrorism, or even treason. Great Britain is one example, where foreign minister Phillip Hammond suggested that British citizens fighting alongside ISIS would be prosecuted for treason upon their return (Morris, 2014). Other countries take a softer approach. The government in Denmark believes that returnees should not be treated as criminals but as victims. They are offered psychological counseling, help to find jobs, or positions in schools and universities (Faiola & Mekhennet, 2014). These efforts are believed to prevent returnees from continuing on their radical path, and reduce recruitment of new travelers. Similar methods were proposed by politicians in the Swedish county of Örebro to prevent returnees from going back to fighting, and to reduce their feelings of alienation (Carling, 2015). Critics believe that it is wrong to reward crimes and that this can lead to perverse incentives. Individuals may reason that there is no risk in going, and on return they are guaranteed a job, which normally can be hard to get. Maybe a combination of policies is possible, where leaving is illegal but citizens who already have returned are offered reintegration support? In any case, something has to be done to address returned fighters, to prevent them from engaging in further terrorist activities and to break the vicious cycle of radicalization in progress.

B. NETWORKS

Terrorist networks are often mentioned in literature and media. But what exactly does the term network mean? This section explains definitions and basic terminology, followed by properties of networks, and the benefits of a decentralized network to a traditional hierarchical organization. In many cases, organizations can be more successful

if they are designed with a network-centric mindset. Even traditionally hierarchical military organizations recognize the need to decentralize their networks.

1. Definitions and Basic Ideas

First of all, what is a network? There are various definitions of what is considered a network and the minimum requirements that a network should have. One definition is that "a network contains a set of objects and a mapping or description of relations between the objects" (Kadushin, 2012, p. 14). Some argue that the minimum requirements that constitute a network are two or three nodes with links between them, while Borgatti, Everett, and Johnson (2013) assert that there do not have to be any ties at all. Simply put, "a network is a set of relationships" (Kadushin, 2012, p. 14).

Every day people are likely to participate in several networks. They can consist of colleagues, family, friends, or club members. Some networks can be in the background and you may not even think about being a member of one, but through your networks, you are able to achieve something you cannot do on your own (Anklam, 2007).

a. Social Networks

Since this paper concerns social networks, terminology and methods from the field of social network analysis (SNA) is used.[4] SNA is concerned with social entities and the linkages between them (Wasserman & Faust, 1994). A *social network* is defined as "a finite set or sets of actors and the relation or relations defined on them" (Wasserman & Faust, 1994, p. 20). The term *network* can be used with different meaning in different contexts. Some distinguish between networks and hierarchies when looking at an organization's structure and topography (Arquilla & Ronfeldt, 2001). In this context, *networks* are considered decentralized and informal organizations, while *hierarchies* are centralized and formal. In the field of SNA, regardless of topography all organizations are treated as networks (Everton, 2012), only more or less hierarchical. This perspective is adopted here, all organizations are called *networks*, and to distinguish between

[4] For three good references on social network analysis, see Wasserman & Faust (1994); Carrington, Scott, & Wasserman (2005); and Kadushin (2012).

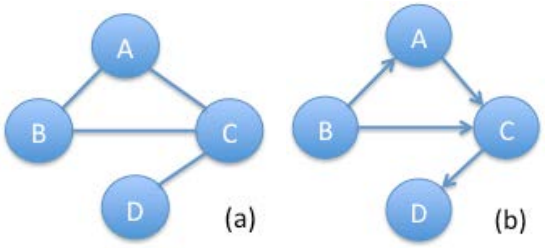
centralized and decentralized networks, Everton's (2012) terminology of hierarchies and heterarchies is used.

Nodes in a social network can consist of individuals, groups, or organizations and are called *actors* (Wasserman & Faust, 1994). The links in a social network represent relationships between the actors and are called *ties*. Ties between actors can represent different kinds of relationships such as kinship or being members of the same club. Prell (2012) distinguishes between *state* relationships and *event* relationships. State relationships have some degree of permanence, like kinship, and are easier to detect for an analyst than event relationships that are more temporary in nature (Prell, 2012, p. 9). Event relationships include talking to someone, attending the same meeting, or participating in a training camp together. Borgatti et al. (2013) describe four categories of relations: co-occurrences (e.g., members of the same club), social relations (e.g., kinship), interactions (e.g., transactions), and flow (e.g., flow of ideas or information).

b. The Nature of Ties

Some ties are directional and some are not; directional ties are often called *arcs*, while non-directional ties are called *edges*. For example, being members of the same club is not a directional tie (see Figure 2a). But when ties represent flow of information or influence, they are directional from one actor to another (see Figure 2b). Both actors and ties have characteristics, often called *attributes*, which can be used to distinguish between them (Borgatti et al., 2013). Attributes of actors can be name, age, or position, while attributes for ties can be type of relationship or time the relation lasted.

Figure 2. Relational Ties between Actors.



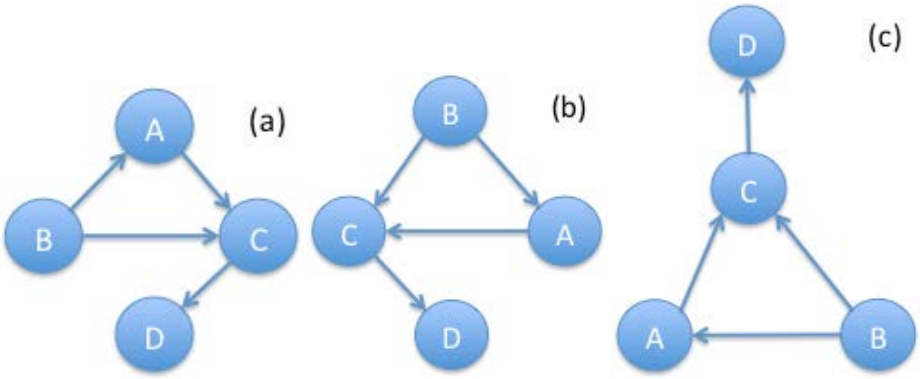
Left (a): Relational ties between actors based on membership in the same club. Right (b): Directional ties (or arcs) illustrating flow of information between nodes.

The types of relationships being studied determine what networks are identified. If kinship is chosen as the relation, a kinship network is displayed, and if friendship is chosen, a friendship network is displayed. Sometimes different relations are combined into an aggregated network to produce a comprehensive picture of various relations between a set of actors. A decision has to be made about what relations are relevant for the specific analysis. For example, kinship, friendship, and interaction relations can be combined to get a picture of how a set of actors are connected. Limitations may also be set by what kind of data or information is available. Kinship is easier to determine than trust, for example.

c. Visualization of Networks

Care must be taken about visualization layout when a network diagram is produced. Figures 3a, 3b, and 3c represent the exact same network, actors, and relationships. Depending on how actors are arranged in the layout, different impressions can be created of which actor is higher hierarchically. Actors should be arranged so that the intended audience easily grasps the point that the diagram is supposed to convey. This depends on which relationship is being visualized. If the ties represent influence, then Figure 3b makes sense with Actor B on top. But if the ties represent flow of money, then Figure 3c is a better representation with Actor D on top. Again, regardless of how the network is visualized, it has the same structure and SNA metrics. Visualization is just a helpful tool to communicate relevant properties to the audience and to assist in analysis of the data.

Figure 3. Visualization of a Network.



The same network is arranged in three different ways to illustrate relative hierarchy between actors.

d. Dark Networks

Terrorist networks are examples of dark networks, or covert and illegal networks (Milward & Raab, 2006). The term *dark* refers to the fact that the network tries to remain hidden. Even though the term is often used for terrorists, criminals, or other gangs who try to conceal themselves and their activities from authorities, the term also applies to networks with good intentions. For example resistance movements during Second World War Nazi occupation would be considered dark networks since they were covert and illegal, according to the occupants (Everton, 2012). A common theme is that these networks try to stay hidden, but why and from whom will vary.

Dark networks experience different design challenges compared to light networks. Structure, roles, tasks, and work processes look inherently different. When analyzing dark networks, it is virtually impossible to get a complete picture of its actors and ties. Members refrain from revealing true information about the network, even if they are captured and interrogated. Sometimes information comes from media or government organizations, but then it must be assumed that information is incomplete, biased, and possibly politically manipulated (Rodriguez, 2005). Data available for analysis are primarily relational; hence relational analysis is appealing for dark networks (Oliver, 2014).

Another contrast to light networks is that different criteria of performance are suitable. Factors like accountability and transparency may be totally ignored in dark networks, and efficiency may be second to perseverance. Oliver (2014) suggests that efficiency, or the capacity to act, are under-theorized for dark networks, as is the concept of covertness. She states that "network capacity and resilience are described as a consequence of several network properties, although empirically these theories remain untested" (Oliver, 2014, p. 7).

2. Properties of Network Organizations

Although there may be significant differences between organizations, "all networks, regardless of their size, shape, or origin, share fundamental properties and insight derived from one type of network transfer easily from one context to another" (Anklam, 2007, p. xiv). With the connectivity that modern information technology offers, information spreads faster and wider than ever before. Since information tends to diffuse faster in a well-connected (decentralized) network (Borgatti et al., 2013), many organizations turn from hierarchical and vertically integrated structures to a decentralized network form to take advantage of partnerships, alliances, and coalitions (Anklam, 2007). Heterarchies will never entirely replace hierarchies as an organizational form (Anklam, 2007); there are some situations where hierarchies are required. One example is certain military contexts where chain of command has to be clear, and strict control is necessary.

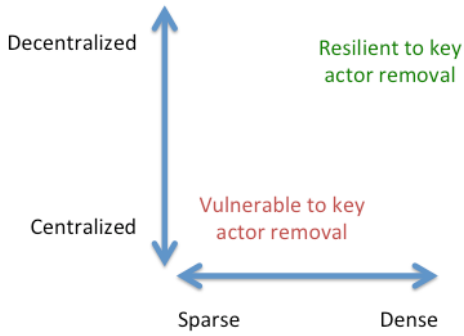
It is not trivial to design an efficient network. Decision-making and governance are examples of central processes that have to be functioning. Networks need to have a clear purpose and direction that members are able and motivated to pursue. By studying the operational environment, it is possible to optimize a network's design to successfully produce the desired outcome.

a. Characteristics

In the field of SNA, where all organizations are treated as networks, two general categorizations can be made. The first measures how hierarchal, or centralized, a network is. The second describes the denseness of the network. A dense network has a lot of strong ties between the actors, while a sparse network has few and weak ties. The first

dimension separates hierarchies from heterarchies, and the second distinguishes between provincial and cosmopolitan networks (Everton, 2012). Everton (2012) suggests that there is an optimum level in both dimensions for every network to be successful depending on the environment it operates in. A highly centralized network has more efficient command and control, but it is vulnerable to the removal of key individuals. A decentralized network is less vulnerable to the removal of key actors but has difficulties in mobilizing resources. If the network is sparse, it can remain hidden more easily because a decrease in communication makes the network less visible to the authorities. But it does not have the same capabilities as a dense network. This argumentation applies to both light and dark networks. If an organization is both decentralized and dense, it is less disrupted when individuals leave (Borgatti et al., 2013), and if a terrorist network is both centralized and sparse, it is more disrupted when a key actor is removed (see Figure 4).

Figure 4. Two Dimensions of a Network: Centralization and Density.



(After Everton, 2012)

b. Group Dynamics[5]

People tend to create connections to other people who are similar on significant social attributes (Borgatti et al., 2013), which results in social formations on different levels. Reinforcement of a group's identity can strengthen bonds and increase resilience. Identity can be built on shared characteristics, symbols, or rituals. If a group is created in

[5] Much of the information in this section was presented and discussed in the course "Trust, Influence and Networks" at Naval Postgraduate School, Monterey, CA, in 2014/Q4.

which members feel like they belong to a certain culture and style, they strongly identify with the group and be less likely to leave. Some groups recruit members by exploiting the human need to belong and to be accepted. Success of recruitment depends on the attractiveness of the group, such as status, reputation, or opportunities for its members. Group thinking can occur where members in a group believe that the existence of the group is important, and they defend the group from external threats. Since members of the group hear the same stories and share the same experiences, a shared reality is created. There is a tendency for group members to conform when confirmation bias is present and external opinions are blocked. It is easy to listen to information that confirms one's opinion and to ignore contradicting information, and it feels good to agree. All this group thinking creates a feeling of "us versus them" where people in the group are trusted and outsiders demonized. This could happen in all types of groups, but it is important to be aware of these dynamics to better understand and disrupt terrorist organizations.

c. Style and Culture

Anklam (2007) describes the style of a network through five key elements: locus, culture, interactions, orientation, and leadership. Locus describes where and how the network operates. Cultural factors of a network include identity, core values, and norms. Interactions in a network can be transaction based, knowledge based, person based, or a combination of the three. The orientation of a network shapes its design, where a network focused on outcome prioritizes production more than a network focused on discovery. Leadership is all about ensuring that members in a network are productive by controlling the other four style elements. Network leaders must be able to sustain networks through holding the collective vision, creating and managing relationships, and managing collaborative processes (Anklam, 2007).

d. A Small World

Every network is a subnetwork of a universal social network through which all persons are connected (Denning, 2011). Human beings have many different kinds of relations and are at least connected with their parents through kinship. If a network is expanded from one individual via all possible kinds of relations, the entire world is

spanned surprisingly quickly. Milgram (1967) conducted his famous small world experiment in 1967 where he asked a sample of individuals to trace their personal relations to a stranger living in a remote city. He discovered that most people were connected to the stranger in six steps or less, which contributed to the popular expression "six degrees of separation."

Homophily is often mentioned in social psychology—the tendency for people to like other people who are similar to themselves on social significant attributes such as age, gender, race, and religion (Borgatti et al., 2013). This phenomenon creates tightly connected, homogeneous groups with strong internal ties. Still, weak ties connecting different groups separated physically, culturally, or socially play an important part in the diffusion of information (Granovetter, 1973):

> Whatever is to be diffused can reach a larger number of people, and traverse greater social distance, when passed through weak ties rather than strong. If one tells a rumor to all his close friends, and they do likewise, many will hear the rumor a second and third time, since those linked by strong ties tend to share friends. If the motivation to spread the rumor is dampened a bit on each wave of retelling, then the rumor moving through strong ties is much more likely to be limited to a few cliques than that going via weak ones; bridges will not be crossed. (Granovetter, 1973, p. 1366)

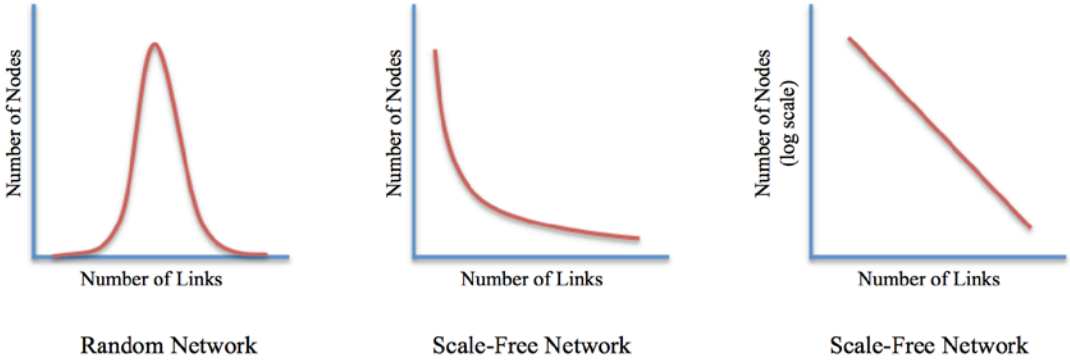
Weak ties connect people and groups around the world and contribute to the six degrees of separation in our small world.

e. Scale-Free Networks

Recent research has shown interesting properties of several kinds of networks thought to be random. The number of connections that nodes have is normally distributed in a random network. On the contrary, many networks share the property that "some nodes have a tremendous number of connections to other nodes, whereas most nodes have only a handful" (Barabasi & Bonabeau, 2003, p. 62). Barabasi and Bonabeau (2003) discuss these kinds of networks, which they call *scale-free*. The authors examine how information diffuses so rapidly in certain social networks and how some networks continue to function even after a large number of nodes have failed. Many complex

networks—including the Internet, cellular metabolism, and certain social networks—contain such important nodes, called hubs, and they all share important characteristics, e.g., they are resilient to accidental failures but vulnerable to targeted attacks (Barabasi & Bonabeau, 2003). Since most nodes have only a few ties, removal of random nodes will most of the time not critically affect network performance. But if one or more of the most important hubs are removed, the network risks becoming fragmented and may not recover (Barabasi & Bonabeau, 2003). More and more scale-free networks have been discovered. How can such diverse systems have the same architecture and properties? Part of the answer is a process called *preferential attachment* where new nodes are more likely to connect to nodes with a high number of existing connections (Barabasi & Bonabeau, 2003). While resilience against accidental failures is a desirable property for networks like the Internet, which still functions even after failure in many routers, the vulnerability of targeted attacks must be addressed. If key hubs are identified, they can be targeted, leading to devastating effects on network performance. For the Internet, it is important to protect key hubs from computer viruses or physical attacks (Barabasi & Bonabeau, 2003). If a terrorist network exhibit traits of a scale-free network, capture of random members have little impact on the network. Instead, the focus should be on identifying key hubs and targeting them. Therefore, it is important to know the topography of the network and determine if it is scale-free to understand its behavior before crafting strategies to disrupt it. Figure 5 illustrates distribution of node linkage in different types of networks.

Figure 5. Distribution of Node Linkage in Random and Scale-Free Networks.



(After Barabasi & Bonabeau, 2003)

C. COUNTERING TERRORIST NETWORKS

Now that the concepts of terrorism and networks have been introduced, focus turns to how governments can work to counter the terrorist threat. First, it is described how the United States has adjusted organizations and methods based on lessons from wars in Iraq and Afghanistan, and from the 9/11 attack. Then it is discussed how methods to disrupt terrorist networks are being developed. Finally, models to analyze terrorist networks to enable successful counter-terrorism strategies are described. This thesis uses the popular SNA approach, but also presents an additional approach, a network design perspective to analyze terrorist networks, in search of strategies to disrupt them. Using the two approaches together could allow for more informed decisions to be made.

1. Organizational Adjustments

In terrorist organizations, networks occur on different levels. A local terrorist cell is one example, with or without connections to a larger terrorist organization. Global al-Qaeda is an example of a much larger network. They all exhibit heterarchical traits such as decentralized decision-making, rapid flow of information and money through the use of information and communication technology (ICT), and a constantly changing structure (McChrystal, 2011). General Stanley A. McChrystal came to realize the challenges that the United States faced during his time as commander in Iraq and Afghanistan. The opposing Taliban network was more heterarchy than army, and fundamentally different

from any previous enemy (McChrystal, 2011). It was impossible to map the enemy in a traditional military structure, as fighters who were adapted to the area made decisions locally, but different groups shared information to allow for coordination and exchange of tactics (McChrystal, 2011). The enemy was organized on the basis of relationships, reputation, and fame rather than rank, and the result was a flexible, self-forming enemy network with an impressive capability to grow and sustain losses (McChrystal, 2011):

> In bitter, bloody fights in both Afghanistan and Iraq, it became clear to me and to many others that to defeat a networked enemy we had to become a [decentralized network] ourselves. We had to figure out a way to retain our traditional capabilities of professionalism, technology, and, when needed, overwhelming force, while achieving levels of knowledge, speed, precision, and unity of effort that only a [decentralized network] could provide. (McChrystal, 2011, p. 67)

U.S. forces did not have the ability to detect and react on indicators rapidly enough to be successful, as the lack of bandwidth and manpower limited the ability to share information efficiently (McChrystal, 2011). There was also a habit in the U.S. military to share only a minimum amount of information, which led to lost or slower information when filtered (McChrystal, 2011). So McChrystal started the challenging process of building a heterarchy by examining what an effective network involves. He concluded that "a true [decentralized network] starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust" (McChrystal, 2011, p. 69). By fusing intelligence and operations efforts, together with culture, into united efforts, intelligence traveled faster up the chain of command and returned in time for those in the fight to benefit from it (McChrystal, 2011). Through a common purpose and by sharing information continuously, U.S. military created a collective consciousness where intelligence recovered on one target would feed both that and other operations (McChrystal, 2011). The number of operations conducted increased, as well as the success rate (McChrystal, 2011). Through decentralizing decisions, removing institutional boundaries, integrating diverse cultures, valuing competency over rank, seeking "a clear and evolving definition of the problem and constantly [self-analyzing], revising its structure, aims and processes, as well as those of the enemy" (McChrystal,

2011, p. 70), an effective heterarchy was created to better match the challenges of environment and enemy (McChrystal, 2011).

In the aftermath of 9/11, it became clear that U.S. counter-terrorism agencies did not perform efficiently. Intelligence agencies did not communicate or cooperate efficiently, which led to vital information being slowed down or lost. Learning from this mistake, a network of organizations was formed where information diffused much more rapidly. Powerful acts of Congress were passed to allow agencies to access and share information to a greater extent. The Privacy Act of 1974 had been posted to limit the government's access to personal information in response to citizens' concerns of a "big brother." A consequence of this act was that agencies did not share information, which may have contributed to the lack of awareness leading up to the 9/11 attacks. In late 2001, the USA Patriot Act went into effect, allowing government agencies greater access to private information. The act has been controversial, and sometimes vague, which has led to protests. The term "reasonable belief" occurs often in the wording, which leaves it up to the courtroom and jury to interpret the act. Hence verdicts vary over time and between courts. Congress was aware that it was acting with the emotional backdrop of 9/11 and set an expiration date for the act at which time the act would be voted on again. The act has since been revised and replaced.

2. Developing Strategies to Disrupt Terrorist Networks

In the war on terrorism, there is a need to craft potential strategies to disrupt terrorist networks. This is a vast challenge, requiring several aspects to be taken into consideration. Often it can be hard to anticipate all the consequences and possible outcomes of an action. Is the targeted network disrupted in the intended way? How do the local population and the U.S. public receive the actions? Are they legally, financially, and logistically possible to execute?

Everton distinguishes between kinetic and non-kinetic approaches, where

> the former involves aggressive and offensive measures designed to eliminate or capture network members and their supporters, while the latter involves the use of subtle, noncoercive means designed to reduce a

> network's effectiveness and impair a combatant's will to fight. (Everton, 2012, p. 32)

Kinetic approaches can be used to target key actors in a network, just as the United States tries to remove al-Qaeda leadership through directed attacks. Non-kinetic approaches try to destabilize networks and to reduce their influence through other means such as "institution building, psychological operations, information operations, rehabilitation and reintegration programs, and the tracking and monitoring of key network actors" (Everton, 2012, p. 34). Some argue that kinetic approaches create more violence and may increase support, determination, and participation of the adversary (Mortenson & Relin, 2006; Everton, 2012). Furthermore, if key actors are removed, depending on the network dynamics, they may easily be replaced. Or, the removal of certain central actors may even make the network harder to track and disrupt (Everton, 2012; Arquilla, 2009). Kinetic approaches may be necessary as a short-term solution, but should be used in conjunction with non-kinetic approaches to support long-term success (Everton, 2012; Roberts & Everton, 2011). When a network is fragmented by kinetic strategies, non-kinetic efforts such as reintegration should be employed to inhibit the network's possibility to recover (Tilly, 2005).

There are at least two fundamental ways that SNA can be used to disrupt networks: to locate critical individuals and for pattern location (Carley, Lee, & Krackhardt, 2002). The authors identify six different characteristics that identify critical individuals:

(1) Individuals whose removal would considerably change the network.

(2) Individuals who are not likely to act on new information.

(3) Individuals who can diffuse new information quickly.

(4) Individuals who are relatively powerful in the network.

(5) Individuals who if they moved to a competing organization would bring all the core knowledge from the first organization.

(6) Individuals who give the network redundancy.

Critical individuals can be identified using a number of different metrics such as centrality, and then targeted by different strategies to disrupt the network. In pattern location, behavior that is different from some kind of standard is sought. This can reveal patterns, or a break of patterns, such as subgroups, tendencies, differences between sets of networks, or different structures between sets of a network (Carley et al., 2002, p. 81). Both ways are used to find potential vulnerabilities that can be exploited to disrupt networks.

Cronin (2009) suggests that rather than a descriptive analysis focused on one group, historical lessons should be used to avoid previous mistakes and to use a broader strategic perception. It is important to avoid "short-term passions in the wake of attacks, and think strategically about dealing with current and future threats" (Cronin, 2009, p. 1). In her book, Cronin proposes analytically studying historical records of how terrorism ends, because the current terrorist threat will end, like all previous ones have (Cronin, 2009). It is not an easy task to end terrorist campaigns. But experience is essential, and many important parallels can be drawn to centuries of practice with terrorism movements. Terrorism has not always looked exactly the same, but "meeting the current threat can best be accomplished by exploiting its classic vulnerabilities" (Cronin, 2009, p. 3). On this note, a network design approach is used here to look at historical terrorist attacks in pursuit of vulnerabilities. Even though some classic vulnerabilities may be the same, each case has to be analyzed in its particular context and the specific environment surrounding the terrorist cell.

A variety of tools are needed to support the decision-making process to determine which strategies to apply. By finding an adversary's centers of gravity, attacks can be directed where the most effect is achieved. Specific desired effects include degrading, destroying, or disrupting the adversary so that they no longer constitute a threat. Two analysis approaches that can inform decision are studied in this thesis: the well-known relational approach of SNA, and an additional approach taken from a network design perspective.

3. Models of Analysis

An understanding of how terrorist networks function is required to craft efficient strategies for disruption. Actions that would have the greatest impact on adversary network performance are determined by analyzing information about the network. SNA is a relational approach that utilizes the empirical study of social relations between actors in a network. Different metrics describe characteristics in the network itself, and among the individual actors, help the analyst to identify weaknesses for exploitation. In this section, a network design approach for analyzing terrorist networks is introduced, which can be used together with SNA to provide greater understanding. This approach may help explaining different relational properties of a network. When the two approaches are used in conjunction, a deeper knowledge of the terrorist network is reached, and more efficient strategies for disruption can be crafted. The two approaches are presented next, to prepare for the thesis analysis model.

a. Social Network Analysis

In the social and behavioral sciences, systematic studies of social systems grounded in empirical and relational data are conducted to analyze behavior. SNA, a collection of theories and techniques which can be viewed as a distinct research perspective within social and behavioral science (Wasserman & Faust, 1994), focuses on how interaction patterns can predict and explain behavior, rather than the attributes of the actors (Everton, 2012). Since social attributes of actors remain the same between different social contexts, they cannot explain why behavior changes in different social contexts. SNA focuses on "relationships among social entities, and on the patterns and

implications of these relationships" (Wasserman & Faust, 1994, p. 3). By using formal concepts and mathematical models with the aid of computers, relations between actors describe the structure of the network and position of actors (Borgatti et al., 2013). Actors are not considered to be autonomous; instead, the behavior of actors is assumed to be dependent on ties to others and the network in which they are embedded (Everton, 2012). Each type of relationship can result in other types; for example, a work relation can lead to a friendship relation (Borgatti et al., 2013). These are two different networks, one friendship network and one work network. It has to be clear what types of ties are being studied. Combining different types of ties creates aggregated networks that give a more complete picture of how a set of actors is interrelated. Ties between actors are seen as conduits that can transfer materials, money, information, or trust (Everton, 2012). Even though SNA has been used since the 1930s, it has evolved slowly until recently (Carrington, Scott, & Wasserman, 2005).

As explained by de Nooy, Mrvar, and Batagelj, "the main goal of social network analysis is detecting and interpreting patterns of social ties among actors" (de Nooy, Mrvar, & Batagelj, 2005, p. 5). An appealing property of SNA is that it can be applied to different levels of networks, from small groups to global organizations (Kadushin, 2012). SNA has helped elucidate the structure of dark networks and can help craft strategies to disrupt them (Everton, 2012). One application is to identify key players to target with kinetic or non-kinetic strategies. While removal of key actors may be tempting, it can be more effective to influence them to change behavior. Studies have shown that changed behavior of a key actor has add-on effects through diffusion to other actors (Borgatti et al., 2013).

SNA methods and theories can be used to describe the structure of a network, identify subgroups, and describe properties of the actors. Some actors have important positions in a network; they can be vital to the flow of information. One important metric is actor centrality. There are variations of how centrality is measured, but they all try to distinguish how central different actors are in a network.

Visualization is an important part of SNA that is used to illustrate results from analysis as well as to aid in the interpretation of data. The human visual system has the

capability to process images and charts much faster than reading descriptions about them (Teerlink & Erbacher, 2006). As explained by Osborne and Slay, "information visualization enables us to connect the language of the eyes; that is shapes, colors and animations with the language of the mind; such as the concepts of relationships, processes, models and behaviors" (Osborne & Slay, 2011, p. 1).

(1) Dynamic Network Analysis

Networks are always evolving and changing; actors enter and leave, and ties form and dissolve (Everton, 2012). Hence the relationship an analyst chooses to study should have at least some persistence, or the ties between actors are too loose. A diagram of a network represents a snapshot—a picture at a point in time. Since networks are always changing, that snapshot may be missing important information; therefore, techniques have been developed to study networks over time, that is, longitudinal networks. Everton and Cunningham went further and analyzed a terror group by using data that takes into account how the group has changed over time (Everton & Cunningham, 2011). This allowed the authors to draw conclusions on terrorist network adaption to a changing environment. This so-called dynamic network analysis can be difficult to conduct, but may offer valuable insights. Dynamic network data may be hard to acquire, and methods to analyze them have been underdeveloped (Everton, 2012). Recent work has begun to change this situation, but the focus of most studies has been on light networks (Everton, 2012). Clearly the concept is promising and may prove helpful in analyzing dark networks in order to disrupt them.

(2) Positional Perspectives and Blockmodeling

Besides studying ties between actors to explain behavior, a positional approach can also be used (Emirbayer & Goodwin, 1994). Instead of focusing on ties between actors, this approach looks at positions in a social structure, and which actors hold similar positions. An example of a position is an accountant; the position is connected to a set of roles (e.g., bookkeeping, handling transactions, and developing budgets), and it is part of a larger social structure of positions (Everton, 2012). Some theorists believe that actors in similar positions have similar patterns of ties and exhibit similar behaviors (Everton,

2012). When two actors have exactly the same relations to all other actors, they are said to be structurally equivalent. A set of structurally equivalent actors is referred to as a *block*, and finding blocks in a network is known as *blockmodeling* (White, Boorman, & Breiger, 1976).

The position of an actor in a network can explain, in part, the possibilities and difficulties an actor experiences; thus, identifying positions is important to predict actor behavior and beliefs (Borgatti et al., 2013). Social resource theory argues that a businessperson who is well connected to actors with great resources is more likely to perform well than someone who can only draw on his own resources (Borgatti et al., 2013).

(3) Integrating Geospatial Information

The integration of geospatial information allows analysts to plot social network data geospatially. This makes it easier to detect patterns that otherwise might have been unnoticed. Additionally, geospatial data allow for geospatially-weighted measures to be calculated. Metrics and visualizations are then geospatially connected and may aid in presenting research results clearly.

(4) Limitations

Roberts and Everton (2011) identify certain weaknesses in the current research on dark networks. One is lack of clarity as to which ties between actors are collected and studied. Researchers should base their analyses on several different kinds of ties to capture the complexity of dark networks (Roberts & Everton, 2011). Roberts and Everton (2005) also claim that there has been too much focus on individual level networks, while the organizational level of dark networks has been neglected. Inter-organizational networks play an important role in, for example, recruitment to insurgencies; hence, further research is warranted in this area (Roberts & Everton, 2011).

Data on terrorist networks are often incomplete and hard to collect (Krebs, 2001). In addition, networks are always changing as members enter and leave (Everton, 2012). If one crucial link is missing because of incomplete data, if the network has changed over

time, or if a mistake is made, the results of SNA may come out very different. Measurements of network and actor characteristics can be heavily distorted, leading to inappropriate strategy proposals. Also, not all observed patterns in a network are meaningful; at least some part of the observed structure is random (de Nooy et al., 2005). As a result, other inputs are needed to support the decision-making process. SNA can be a helpful tool to propose strategies but is not a sole solution.

There is also disagreement about the interpretation of data on dark networks, possibly resulting from different exogenous factors such as data used, context, and approach (Oliver, 2014). Several studies are contradictory as to the characteristics of a dark network in terms of density, centralization, and other dimensions; one reason is the flexibility, or lack of agreement, regarding the terminology used (Oliver, 2014). Therefore, it is important that analysts clearly define what is meant by a "network," a "strong tie," or a "weak tie."

b. A Network Design Approach

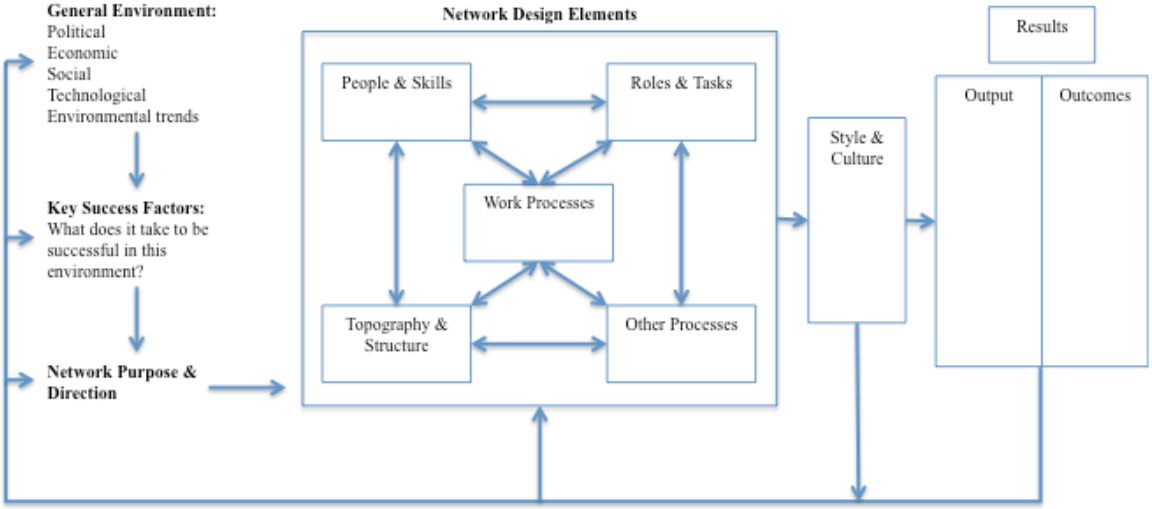
In this section, an additional way to analyze dark networks is introduced. Taking a network design approach enables analysis of how networks organize activities and tasks, use technology, apply leadership, utilize skills, and manage various processes. Network design can be seen as a theory for determining which structure is most efficient in a particular situation/environment. That may have important merit in explaining why networks are successful or not. It is an additional approach to study how to manage a terrorist cell, because it is a management challenge. Someone actually takes leadership and configures a network. To define the thesis research model, a framework is needed to describe and analyze networks from a network design perspective.

Roberts (2003) has developed an organizational system's framework that can be used to describe networks as systems, and analyze their performance. A variant of this framework, introduced in a network design class at Naval Postgraduate School,[6] is used here (see Figure 6). The framework portrays key aspects of a network, how those aspects are related, and how the components function as a whole. The process starts with an

[6] The framework was used in DA4620 Network Design, 2015/Q3.

examination of the general environment; this is something static that cannot be changed.[7] What is required to be successful based on the specific environment is identified, and the network is designed accordingly. With a suitable design, results of the network match purpose and goals. Here the framework is used to investigate under what conditions terrorist networks were successful to be able to deny future terrorists those conditions. The framework can also be used to increase performance in your own networks by designing them well. It is a descriptive model, in which issues in each element are discussed, as well as how they fit together as a whole and with the environment.

Figure 6. Roberts's Network Design Framework.



(After Roberts, 2003)

(1) General Environment

The first step is to study the general environment that the network operates in, including political, social, and technological aspects as well as environmental trends. It is assumed that the external environment affects the network, and that there is a constant interaction between the two (Roberts, 2003). The goal is to keep the network design in alignment with the environment. In U.S. Army operational planning, the following

[7] It would take a lot of time and resources to change the general environment. The network design analysis in this thesis does not look at a network over such long periods of time. One possibility for an organization is to choose to operate in an environment that is promising, but this is not always an option.

environmental variables are considered (PMESII-PT): political, military, economic, social, information, infrastructure, physical environment, and time (U.S. Army, 2011). Each of those variables will be described in this research.

(2) Key Success Factors

Next is the identification of what it takes to be successful in this specific situation, based on the environment study. Some things are similar between different contexts, but certain explicit details may explain what would make an organization successful in a particular environment.

(3) Network Purpose and Direction

This can also be referred to as the orientation of the network—the values and beliefs that the network promotes, and the goal of the network. At this point, goals, values, and beliefs are espoused and do not necessarily depict what actually occurs in the network. The direction is a guide into the future, outlining network mission, vision, and objectives (Roberts, 2003).

(4) Network Design Elements

Networks consist of several interdependent parts, and these are the key elements that should be configured to allow success in the given environment, and to produce a result that matches purpose and direction (Roberts, 2003). The elements should be "well aligned and fit together. Misaligned parts reduce system efficiency and effectiveness" (Roberts, 2003, p. 1).

- People and skills: Members is one of the most important assets to a network. This network design element lists people in the network, and their skills, knowledge, and abilities (Roberts, 2003). A network does not perform well without appropriate skills. Motives and mindsets of members can also be included in this part of the description.
- Roles and tasks: This is a description of important roles and tasks in the network. Leaders and managers are essential roles in all networks (Anklam, 2007). It includes basic tasks that people are expected to perform, how formalized the tasks are, and how the tasks are differentiated (Roberts, 2003).

- Work processes: Work processes are related to how the work gets done, and includes everything that directly leads to output being produced. It can be seen as a description of "how the organization produce outputs through the various tasks it does" (Roberts, 2003, p. 3).

- Topography and structure: This is a tangible facet of the network, where a description of how the network is structured can be drawn. Both organizational form and internal connections are relevant. Terminology and methods from SNA are used in this part. The level of centralization is considered, as well as division of labor, and the structural coordination and integration of subgroups (Roberts, 2003). How decision-making is distributed can also be considered a structural aspect.

- Other processes: Here, processes that support the network so that work processes can function are described, i.e., planning and decision-making processes, information management and communications, human resource management, and financial management (Roberts, 2003).

(5) Style and Culture

Style and culture are emergent properties, which stem from how the network is functioning. Here the actual behavior of the network is described as compared to espoused values, how "people interact and behave toward one another, and how they manage their differences" (Roberts, 2003, p. 5). It is important to examine whether there is a distinction between espoused beliefs and how people actually act, which may lead to tensions that can be exploited. The existence of subgroups and subcultures may also affect performance if the network does not share the same goal.

(6) Results

Finally, performance results are described to measure how successful a network is, because "operational outputs provide feedback to judge organizational performance" (Roberts, 2003, p. 1). There are many different ways to measure results, and what is considered important is likely to differ between various stakeholders in the network (Anklam, 2007). Roberts (2003) distinguishes between outputs and outcomes:

- Output: Outputs are tangible and measurable results such as goods or specific services produced by the network. The output from a terrorist attack can be number of casualties.

- Outcomes: Outcomes are consequences of outputs, and can sometimes be much more important than actual output. It can be hard to measure outcome, and hard to predict or anticipate. The outcome of a terrorist attack can be that a state changes its national security policy.

D. SUMMARY

Knowing an enemy well increases the likelihood of defeating that enemy. This chapter described existing research on the topics of terrorism, networks, and counter-terrorism methodology. General properties of terrorist networks were covered, followed by a discussion of recent attacks and current issues. The field of network theory was next briefly introduced, including social network theories and terminology.

Learning from recent terrorist attacks as well as wars in Iraq and Afghanistan, the United States has made adjustments to organizations, methods, and laws regarding counter-terrorism. Analysis of the adversary suggests that a decentralized network approach should be taken to counter this networked threat. There are different models for analyzing networks; SNA is a powerful empirical relational approach. But SNA is just a way to craft strategies; it does not answer which strategy to choose (Everton, 2012; Roberts & Everton, 2011). The decision-making process is more complicated than that, and must be dependent on context. Endogenous and exogenous factors affect the interpretation of SNA metrics. Here the additional network design approach can help by providing context to the results from SNA.

Roberts's network design framework has been introduced, and is used in this thesis to analyze historical cases. The research design in Chapter III describes how SNA and a network design approach are applied in pursuit of strategies to disrupt terrorist networks.

III. RESEARCH DESIGN

This chapter describes how the thesis research is conducted. Building on theories and concepts described in Chapter II, this study is intended to provide additional explanatory value of how to disrupt dark networks. By collecting historical information on terror groups, and then structuring and analyzing data, insights can be gleaned regarding the added value of the network design approach. The network design model is used together with social network analysis (SNA) to analyze two cases, one in which the terror group was successful and one in which it was not. After describing how the research is designed, potential errors in the model are discussed.

A. CASES FOR ANALYSIS

The first case is the Madrid 2004 train bombings, which led to Spain withdrawing its troops from Afghanistan. Even though the terrorists were successful, there were still network design problems to learn from. This case is selected because of its significant outcome, and the quality and volume of publically available information on it. The second case is the Toronto 18 terrorist group, which plotted attacks in Canada between 2005 and 2006 but was destroyed by a coordinated counter-terrorism operation in June 2006. This case is selected because it is a good example of a terror group that failed because law enforcement agencies successfully intervened before any attacks could be performed. Both cases are taken from Western countries around the same time, but the environments are not similar enough to control for situation of context. Since the general environment and network goals differ between the cases, the different results cannot necessarily be explained by the network internal design. But in this study, the purpose is not to compare the two cases; the two analysis models are compared to see what explanatory value they provide in different situations.

B. DATA COLLECTION

There is a lot of publically available information to use in both cases. A number of papers, books, and articles have been published on both groups. Data are collected for analysis by studying these historical records. Since the purpose of the research is to

evaluate the analysis models rather than examining a specific case, the data do not have to come from a primary source. Primary sources are preferred in any scientific study, but in this case, the secondary sources are acceptable. Even though data may be biased or incomplete, applicable data are available to inform the two analysis models. The study shows how the two analysis models can be used to analyze networks, and to identify strengths and weaknesses that can be targeted. The purpose is to show how the models can be used in a generic case.

The analysis is focused on a snapshot in time, even though networks constantly change and evolve. Data are collected about how the networks were configured at the time of the attack, or at the time of disruption. It can be valuable to perform dynamic network analysis to learn how group change over time, but this thesis is focused on the critical point in time when the network succeeded or failed. That is a defining moment for each group, when they have reached their performance phase (Anklam, 2007).

Other researchers have performed SNA on the two groups, and their results are used to describe the groups. Interesting conclusions have already been made from SNA on the groups, and potential strategies that would have disrupted them have been proposed. By adding the network design perspective, added value is shown, and how it may assist in the development of strategies to disrupt terrorist networks.

C. DATA STRUCTURE

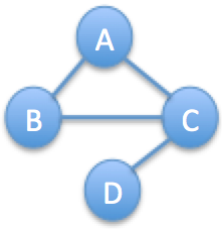
Relational data are coded so that they can be used by SNA software such as UCINET, Netdraw, or ORA.[8] Networks can be represented in relational matrixes, where a basic network type is an undirected dichotomous network. An undirected network has only edges and no arcs, and dichotomous means that the presence or absence of a tie is represented by a "1" or a "0." For each type of tie studied, a relational matrix is produced where the actors in the network are represented by one column and one row each. The intersecting cells indicate the existence or absence of ties. When a relation exists between two actors, the intersecting cell contains a "1," and when no relation exists, the

[8] For more information about the software, see the corresponding website: https://sites.google.com/site/ucinetsoftware/home/, https://sites.google.com/site/netdrawsoftware/home/, and http://www.casos.cs.cmu.edu/projects/ora/.

corresponding cell contains a "0." In situations where relations are assigned various strengths, numerical values can be used in the matrix instead of only ones and zeros. The matrix is symmetrical when ties are undirected. A relational matrix is illustrated in Figure 7, along with the corresponding network diagram. The diagonal in the matrix can be undefined like in the example, or have meaning; it depends on the type of tie being recorded. Relational matrixes like this are read into analysis software, which then can calculate a number of metrics on the networks as well as visualize them.

Figure 7. Relational Matrix with Network Diagram.

	Alice	Bob	Charlie	Daisy
Alice		1	1	0
Bob	1		1	0
Charlie	1	1		1
Daisy	0	0	1	



Each "1" in the matrix represents a tie between the actors on the respective row and column. The ties link actors together in the diagram. Notice how the matrix is symmetrical in the case of undirected ties.

For the network design analysis model, collected data are structured using the network design framework described in Chapter II to provide a conceptual map for each network. When collecting historical records of the groups, information is recorded into the appropriate parts of the framework. Key elements of the networks, as well as external factors, are identified and described by structuring the information according to the framework. This enables a methodical analysis, as well as comparison between different cases.

D. DATA ANALYSIS

After data are collected and structured, the two analysis models are applied. Each model has merit, but they provide different information. While the output of SNA is empirical in nature, the output of the network design model is more descriptive. SNA provides specific values, rankings, and categorizations based on empirical data, which can be used to identify vulnerabilities to exploit such as removal of central actors, or

filling structural holes (Burt, 1992). Network design analysis offers a different way to think about methods for disruption; there is also a network design perspective to find a way in. Keeping a terrorist network operational is a leadership challenge that requires an appropriate network configuration to achieve the purpose in a given environment. In addition, the network design approach may be used to explain results from SNA, including why metrics vary over time. It can validate strategies derived from SNA, or offer insights that lead to strategies being rejected. The network design approach is not intended to replace SNA; it is just an additional tool to inform the decision-making process.

1. Social Network Analysis

It can be challenging to define network boundaries in SNA, because networks are evolving and changing, and boundaries can be fuzzy (Krebs, 2001). It has to be decided who to include in the network and who to leave out. In some situations it is simple, as when looking at members of a legitimate club with a public members list, but sometimes there can be more uncertain boundaries of a network, as is often the case with dark networks. Hard as it can be, "accurately specifying a network's boundaries is of the utmost importance. Misspecification can lead to the incorrect estimation of metrics and the development of inappropriate strategies and recommendations" (Everton, 2012, p. xxviii). Boundaries in this research are defined depending on available data. Network boundaries are clearly defined in each studied case so that all members match a certain criteria, forming a census sample (Borgatti et al., 2013). When the boundaries are set, the analysis is a whole-network type where ties among all set of nodes are studied, rather than an ego-network type where a set of focal nodes and their ties to others are assessed (Borgatti et al., 2013).

One mode interpersonal networks are studied here, with individuals as the only actor type. To capture the complex picture of how actors are related, several types of ties are analyzed. Again, which ties are possible to analyze depends on the available data, but it has to be clear which types of ties are being considered (Roberts & Everton, 2011). All of the following categories of ties can be studied individually or be combined in an

aggregated network: co-occurrences, social relationships, interactions, and flows (Borgatti et al., 2013).

SNA software is used to calculate a number of metrics, including actor centrality, cohesive subgroups, and brokers and bridges.

The field of network analysis has developed a collection of formal concepts to characterize structure and positions in networks, and computers can analyze large amounts of data (Borgatti et al., 2013). This mathematical approach can be measured and codified, which provides formal results about the studied network. Some values may be misleading or incorrect, especially when analyzing incomplete data about dark networks. That is why the network design approach is proposed as an additional tool to inform decision-making by looking at a larger set of network factors.

2. A Network Design Approach

The network design framework described in Chapter II is used when taking the network design perspective to analyze the two historical cases. Network design can be viewed as a theory for determining which configuration is most efficient in a particular situation/environment. First, the general environment where the network operates is described, and then key success factors in that specific environment are identified. Network performance and results can be explained by studying how well the network is configured for the specific environment and network direction. Internal network configuration affects the performance of the group; there may be built-in design tensions where different network design elements are not aligned with each other, with the environment, or with the network direction. If there is a difference in the emergent culture of the network compared to the espoused values and beliefs, there is a misalignment that may be exploited. Another design tension that affects network performance occurs if there is too much focus on work processes, and other supporting processes are neglected. Other questions addressed in the network design analysis are whether the group has the required people and skills, and how well they are organized into roles and tasks. This is a leadership issue and lack of good leadership inherently results in poor organizational performance.

By analyzing groups from a network design perspective, it becomes apparent why they are successful or not in their operating environment. The goal is to identify weaknesses and strengths that can be targeted. The network design framework was developed to find weaknesses and strengths in an organization to improve performance, but it can also be used to discover how to reduce performance. That is the goal of this thesis, to find strategies to disrupt terrorist cells by adding the network design perspective to the analysis.

E. POTENTIAL ERRORS

When analyzing dark networks, it is expected that data are incomplete. There are also problems with fuzzy boundaries, and networks are constantly changing and evolving (Krebs, 2001). These three issues potentially introduce errors in the research. Data in this study are mainly taken from secondary sources and cannot be confirmed. Borgatti et al. (2013) specify four types of errors of concern in SNA: omission errors, commission errors, tie/node attribution errors, and data collection and retrospective errors. The first two types involve how to select ties or nodes, which can have a huge impact on network metrics. The third type results from assigning attributes to ties or nodes incorrectly, and the last type is concerned with how questions are formulated in the data collection phase. All four types of errors are possible in this research; it is essential to be aware of them and to take care to minimize errors.

Data from our two cases are only used for illustrative purposes, to show how the two approaches can be used. The purpose is not to develop specific targeting packages for these cases. To ensure accurate data and valid analysis, two well-known cases are studied for which a lot of information is available and detailed studies have been conducted.

F. SUMMARY

This chapter has described how research was conducted. Two historical cases have been selected for a comparison between two analysis models: SNA and a network design approach. The first case of study is the Madrid train bombings in 2004, and the second is the Toronto 18 terror group that was active in Canada between 2005 and 2006.

The first group achieved their goal while the second failed. In both cases, there is a lot of information publically available, and historical data are collected from published papers, books, and articles.

Collected data are structured into relational matrixes for SNA and structured using the network design framework for network design analysis. The two approaches are applied to see what different explanatory value they have in analyzing dark networks. Better strategies to disrupt terror groups are pursued by using the two approaches together. Incomplete data or incorrect specified boundaries of the networks may lead to erroneous conclusions for both analysis models. To avoid this, two well-known cases have been selected for study.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS

This chapter presents the results of the analyses. First, the two different cases are introduced. Then both are examined, first, using social network analysis (SNA) and second, the network design approach. The SNA builds on previous research on the groups, and the network design approach adds explanatory value by looking at a bigger picture.

A. CASE 1: THE MARCH 11, 2004, MADRID BOMBINGS

On March 11, 2004, a Western country experienced the worst terrorist attack since 9/11 when several bombs were detonated on trains in Madrid, Spain. The terrorist cell, with ties to al-Qaeda, killed 191 civilians and injured more than 1,500 (Rodriguez, 2005). The attacks made Spain withdraw from Iraq, exploiting a sensitive political situation with general elections only days away. This case is important because the terrorists successfully reached their goals, and there are several interesting properties in the terrorist network that can be learned from. There has already been several important studies of this case (Garcia-Abadillo, 2004; Reinares & Elorza, 2004; Rodriguez, 2005), but a network design approach has not been applied. The name *March 11* will be used to refer to this network in the remainder of the thesis.

Network boundaries in this case are the same as Rodriguez (2005) used in his analysis, which is suitable since the SNA that follows builds on his work. The network consists of 70 actors, connected by various types of ties. The part of the network that actually conducted the attacks consists of 13 actors, with the remaining 57 actors serving as a support network.

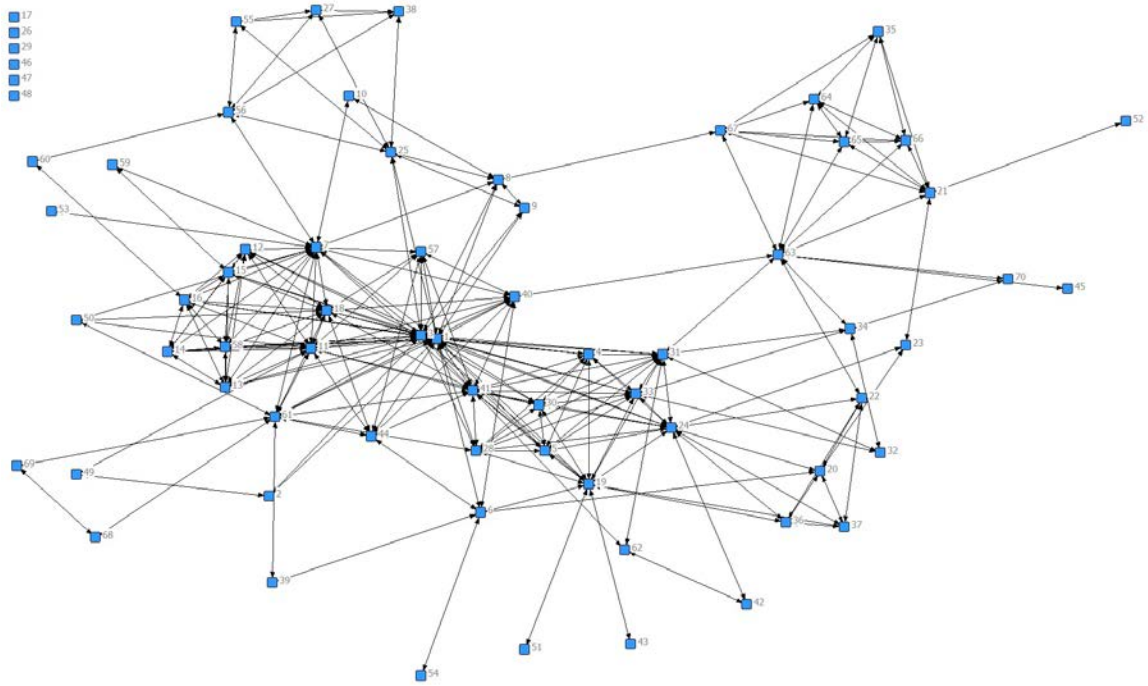
Rodriguez presented detailed SNA of the March 11 network in 2005, where he uncovered the network by mapping relations between the actors. Various techniques from SNA were used to analyze and visualize the terrorist network, which provided several insights. One key finding was the importance of weak ties that dominated the network. Rodriguez (2005) stated that weak ties provide terrorist cells with operational ties to larger networks from which support in the form of supplies or guidance can be drawn. In

addition, weak ties provide “three additional advantages over strong ties for clandestine terrorist groups: 1) they give them stability in the face of arrests or mission failures, 2) they confer flexibility, so that last minute adaptations can be made, 3) and security, in that they remain largely invisible to police forces” (Rodriguez, 2005, p. 2).

To remain hidden is a key success factor for most dark networks. Not only may their planned attacks be stopped if they are exposed, the very existence of the network is at stake (Rodriguez, 2005). Rodriguez’s (2005) study revealed structural characteristics that allowed for the network to remain undetected while sustaining coordination during the preparation of the attack. The network was largely built on personal knowledge and trust based on previous relations, and strong ties were forged before the terrorists arrived in Spain through participation in training camps and wars (Rodriguez, 2005). While in Spain, the network could benefit from these existing ties and required less interaction, which helped them to avoid counter-terrorism agencies.

Rodriguez (2005) maps relations of three types: binding ties, repeated encounters, and reliability. Binding ties include kinship and friendship, while reliability is based on connections to international terrorist networks or participation in training camps and wars. These ties were aggregated in this thesis to get a comprehensive picture of the complete network, which is illustrated in Figure 8.

Figure 8. The March 11 Network.



(After Rodriguez, 2005)

The network proved to be highly segmented into different clusters, with different skills, tasks, and even leaders (Rodriguez, 2005). Inter-cluster communications were minimized to reduce risks of detection and disruption (Rodriguez, 2005). Only 12% of the ties were strong; the network was essentially based on weak connections (Rodriguez, 2005). This arrangement of weak ties is what made the network function; it allowed communications with little effort and low social cost, as central players were able to communicate to most actors in few steps, and resources could be drawn from international terrorist networks (Rodriguez, 2005). According to Rodriguez (2005), trust-based relations built on interaction were the most important type of tie for the creation of the network.

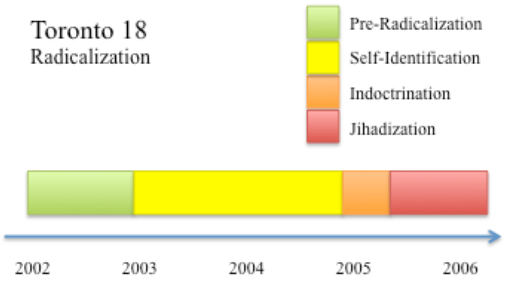
B. CASE 2: TORONTO 18

The Toronto 18 terror group consisted of young American and Canadian men who planned terrorist attacks in the Greater Toronto Area (GTA) between 2005 and 2006. They were all Muslims and were torn between two different worlds made up of "the

traditional culture of their ethnic heritage and family, and the youth culture of the dominant society in which they lived every day" (Bramadat & Dawson, 2014, p. 81). The group was completely destroyed by a police operation starting on June 2, 2006.

The group consisted of two clusters, one in Mississauga, a suburb of Toronto, and one in Scarborough, a neighborhood in Toronto (Silber & Bhatt, 2007). Members attended mosques where they experienced a fellowship that they lacked in the outside world (Bramadat & Dawson, 2014). Various problems were blamed on the government, and sympathy grew with Muslims suffering around the world because of Western powers (Bramadat & Dawson, 2014). They became increasingly alienated from their previous lives and "formed a group of like-minded individuals in a quest to strengthen [their] dedication to Salafi Islam" (Silber & Bhatt, 2007, p. 33). In 2005, they started plotting several attacks where they would target the Parliament, Canadian Security Intelligence Service, the stock market, and a military base, to avenge Muslims killed abroad and end Canada's involvement in Afghanistan (Bramadat & Dawson, 2014). The group had been under surveillance for some time and was successfully infiltrated by two informants. This allowed police and security agencies to conduct a series of raids that led to the arrest of most members. Figure 9 illustrates an estimation of the radicalization process of Toronto 18.

Figure 9. Radicalization of the Toronto 18 Terror Group.



(After Silber & Bhatt, 2007)

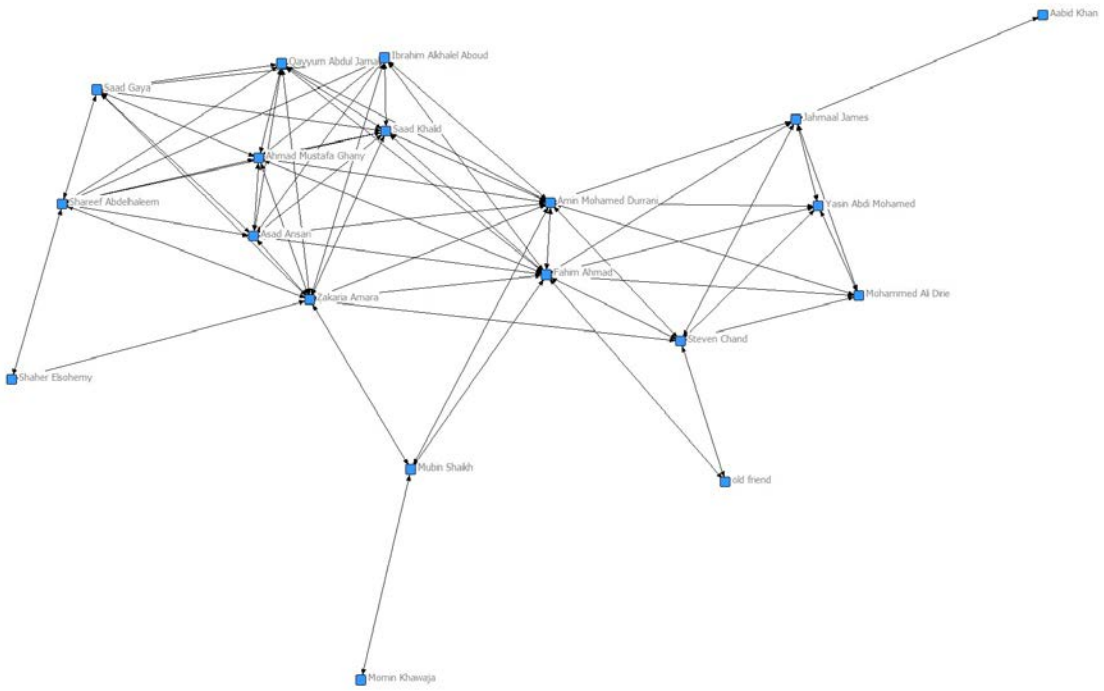
French (2013) collected data on Toronto 18 from a series of articles published by the *Toronto Star* that were based on court documents and information from security services. Twenty-three individuals were included in that material, but there was limited

data on four of them since they were youths. The remaining 19 men are included in this analysis, and that sets the boundaries for this case. These 19 individuals include the following: 10 men who were sentenced after the police raids, four men who were arrested but not convicted, two informants, one man already in custody, one British citizen who arranged access to training camps in Pakistan, and a fraudster who could assist in bank schemes to get funds (Bramadat & Dawson, 2014; French, 2013; Silber & Bhatt, 2007; Teotonio, 2010).

The data French collected in 2013 were recorded in relational matrixes describing the following types of ties: kinship, friendship, affiliation, finance, links, and recruitment. There were also two-mode networks linking actors through shared schools, mosques, vehicles, residences, and weapons. Here the relations were aggregated in order to show a somewhat comprehensive picture of how the actors were connected.[9] The resulting network diagram is shown in Figure 10, where strong ties are represented by thicker lines than weak ties.

[9] UCINET was used here to manipulate data, and to visualize the results.

Figure 10. The Toronto 18 Terror Group.



(After French, 2013)

C. SOCIAL NETWORK ANALYSIS

UCINET, Netdraw, and ORA were used to calculate a number of metrics on both networks. SNA offers a variety of metrics to describe the network and its actors from different perspectives. The first topic covered here is network topography, and then the focus shifts to actor-specific metrics. It is important not to rely on one single metric, which may be misleading; therefore, several different metrics are calculated to provide a comprehensive picture.

1. Network Topography

In this section, metrics describing network topography are considered. Basic features like size and diameter are complemented by more advanced metrics that can describe where the network is positioned in the two dimensions introduced in Chapter II: centralization and density. In addition, subgroups and clusters are identified to highlight factions within the network.

a. Basic Metrics

Table 1 presents basic characteristics of the two networks. The values can be informative alone, but more importantly, they can be used in conjunction with other metrics:

- Size: Network size is defined as the total number of actors.
- Diameter: This is the furthest any two actors are separated, considering only the shortest paths between each pair of actors.
- Average path distance: This is the average separation between each pair of actors.

Table 1. Basic Topography Metrics.

Metric	March 11	Toronto 18
Size	70	19
Diameter	6	4
Average path distance	2.658	1.860

These metrics provide us with some basic facts that are considered when other metrics are interpreted. It is natural that diameter and average path distance is higher for March 11 than Toronto 18, since it is larger.

b. The Hierarchical–Heterarchical Dimension

In this section a number of metrics are calculated to determine how centralized the networks were. Before calculating centralization, the networks were dichotomized to get a value between 0–100%. If the data have other values than just ones and zeros, scores can become higher than 100%. The following three different metrics, calculated using UCINET, Netdraw, and ORA, are presented in Table 2:

- Centralization: There are different implementations of centralization calculations, using the difference in centrality scores between actors, as compared to the highest one, to estimate the level of network centralization. As seen in actor-based metrics, there are several different ways to measure actor centrality. In this paper betweenness centralization is used, which Everton (2012) suggests best matches our intuitive understanding of centralization.

- Variance: Variance is similar to centralization, but compares individual actors' scores to the average value rather than to the highest score.

- Standard deviation: The square root of variance is called standard deviation. This value relates better to centralization, since variance is calculated using the square of the differences between individual scores and the average value (Everton, 2012).

Table 2. Centralization Metrics.

Metric	March 11	Toronto 18
Centralization	14.63 %	21.04 %
Variance	7635.371	128.064
Standard Deviation	87.381	11.317

The first metric in the table indicates that Toronto 18 is more centralized than March 11, but the other two metrics suggest the opposite. Hence no clear conclusion about which network is more centralized can be made. Dark networks have been described as both centralized and decentralized; there is a design conflict between protecting leaders and being able to access members to lead a network (Oliver, 2014).

c. The Provincial–Cosmopolitan Dimension

The second dimension of a network's topography can be evaluated through a series of metrics. The following values are summarized in Table 3; each gives an indication of how dense the networks are:

- Density: Network density is measured as the ratio of existing ties compared to all possible ties. For a full mesh, the density is 1.0, and the density is 0.0 if there are no ties at all.

- Average degree centrality: Density tends to decrease when network size increases; therefore, average degree centrality (the number of ties actors have on average) is a better metric for comparing networks of different sizes (Everton, 2012).

- Clustering coefficient: Also known as ego-centrality, the clustering coefficient is estimated by averaging the density of all actors' ego networks, that is, each actor's direct ties to other actors, and the ties between them.

- Fragmentation: Another metric that describes cohesion is fragmentation (its additive inverse is called cohesiveness). It measures the proportion of

pairs of actors that are not connected, either directly or indirectly. For Toronto 18, the network consists of only one component, so the fragmentation is zero. But there is a distance-weighted variant that takes the path length between all pairs of actors into account. This metric can be useful when analyzing how the removal of nodes would affect a network.

Table 3. Density Metrics.

Metric	March 11	Toronto 18
Density	0.100	0.380
Average degree centrality	6.886	6.842
Clustering coefficient	0.666	1.870
Fragmentation (distance-weighted)	0.625	0.348

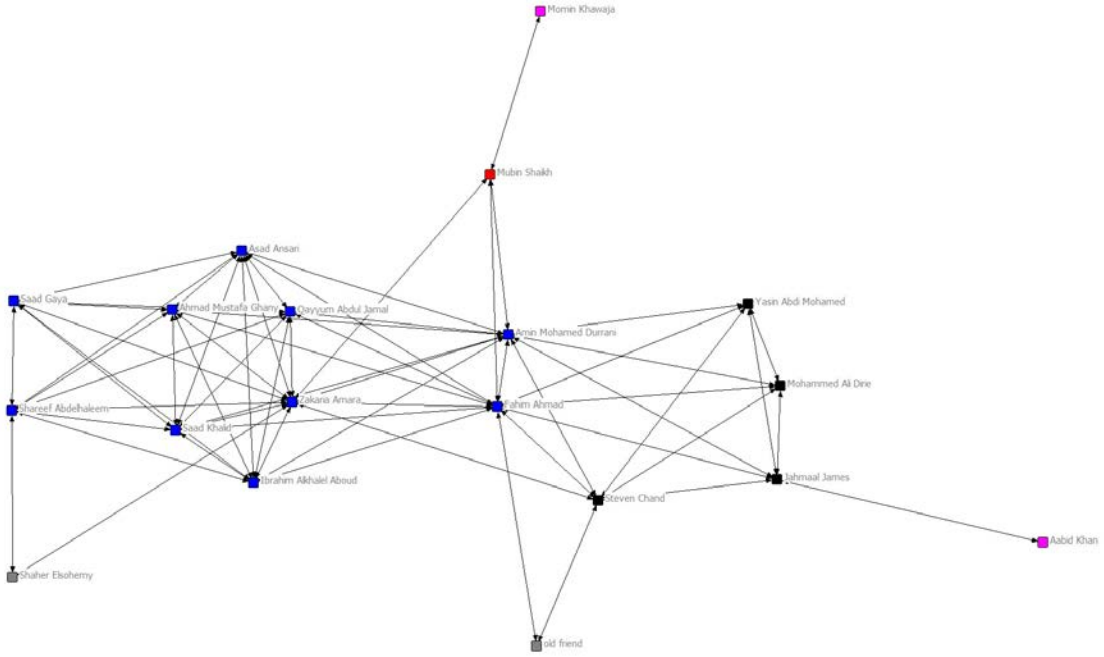
The density value for March 11 is less than for Toronto 18, but this is expected since the network is larger. Average degree centrality is more suitable to compare density between networks of different sizes, and those values are almost identical. The clustering coefficient is higher for Toronto 18, and the fragmentation is lower, both indicating that Toronto 18 is the denser network. Since March 11 was disconnected with several isolates, a higher fragmentation is anticipated; the standard fragmentation score was 0.165 as compared to zero for Toronto 18. Considering the several isolates in March 11, the high average degree centrality suggests that there are some actors with high degree centrality who bring the average score up. The defining characteristics of a dense or sparse network, and the "normal" values for dark networks are debatable. Oliver (2014) compared a series of dark network studies, and the authors had different opinions of what is considered dense or sparse. The metrics can preferably be used to compare and contrast networks, but caution must be taken as to what ties are being analyzed in the different cases, and the quality of data available.

d. Identifying Subgroups

Another important part of network structure analysis is to identify different cohesive subgroups. Cohesive subgroups are "subsets of actors among whom there are relatively strong, direct, intense, frequent, or positive ties" (Wasserman & Faust, 1994, p. 249). One approach is to cluster actors based on similar attributes, but here clustering is based on relations.

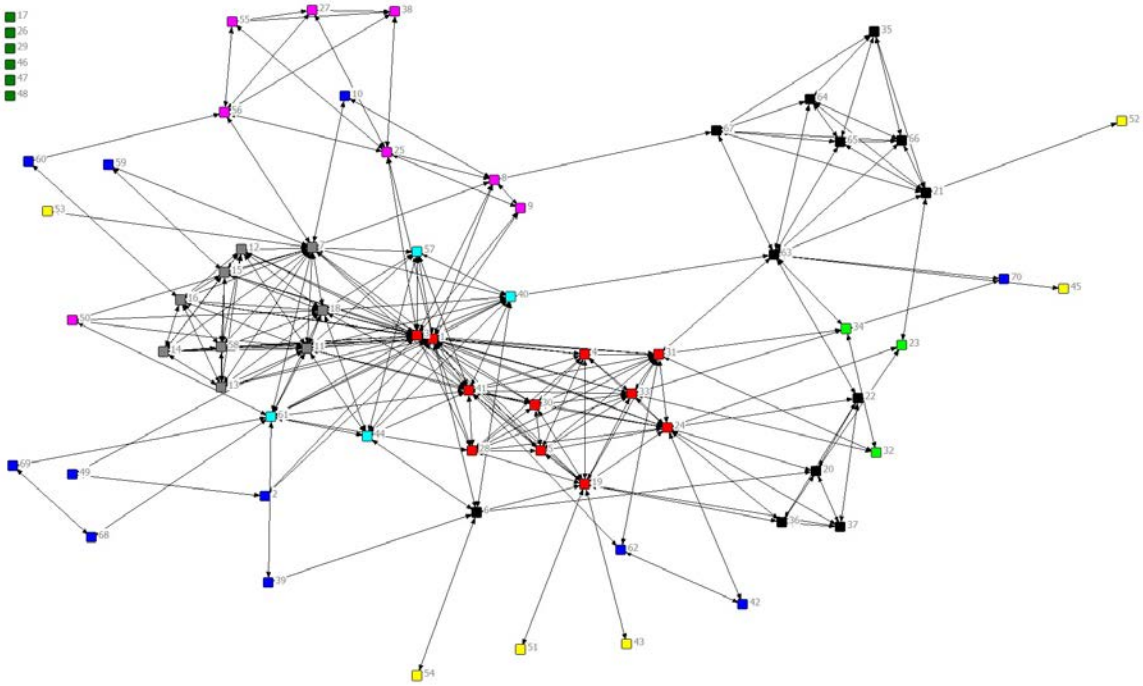
First, k-cores were identified to locate cohesive subgroups. This metric specifies the minimum number of ties that actors have in each core; for example, a 3-core includes actors who all have at least three ties to each other. The highest k-core in Toronto 18 had at least seven ties between all actors, and included 10 actors. There were larger k-cores in March 11, with a maximum of 10 ties. Figure 11 presents all k-cores in the Toronto 18 network, and March 11 k-cores are visualized in Figure 12.

Figure 11. K-cores in Toronto 18.



(After French, 2013). Blue actors have at least 7 ties between them, black have 5, red have 4, grey have 3, and magenta have 2.

Figure 12. K-cores in March 11.

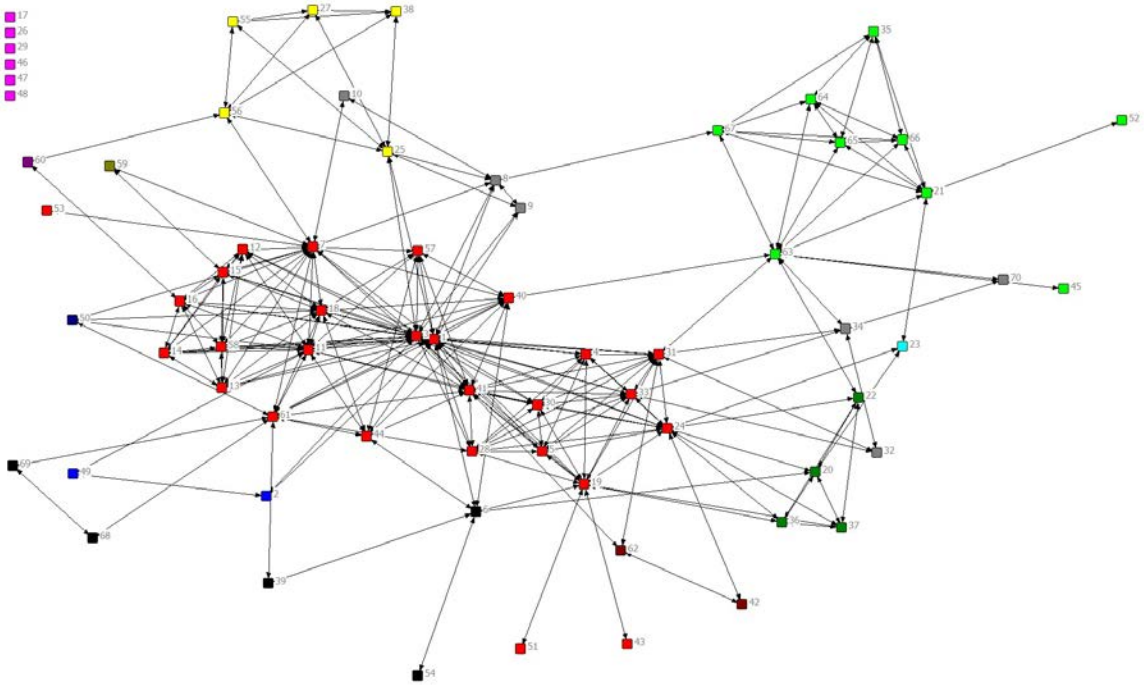


(After Rodriguez, 2005). Red actors have at least 10 ties between them, grey have 9, turquoise have 7, black have 5, magenta have 4, light green have 3, blue have 2, yellow have 1, and dark green have 0.

Next, actors were partitioned into factions, and the fit of the partitions was measured. The optimal partition of Toronto 18 actors into factions was calculated using different algorithms in UCINET and Netdraw, but no clear subgroups could be detected. Division into four, five, six, or seven factions each received the best fit depending on the algorithm used. The calculated fit was similar in all these configurations.

For March 11, the best fit was generated when splitting the group into 14 or 15 factions, depending on the algorithm. This indicates that there were several small factions with limited connections to each other. A division into 14 factions is visualized in Figure 13, with each faction represented by a different color. There is one central faction, with several peripheral factions around it.

Figure 13. Factions in March 11.



(After Rodriguez, 2005). Each faction is represented by a different color.

2. Actor Metrics

Now metrics that describe properties of actors will be calculated. Common approaches include studying how central actors are, how well they can broker information, and how constrained they are by their ties. All three perspectives are discussed here.

a. Actor Centrality

There are several different ways to measure actor centrality. Four centrality metrics a calculated here and the same five actors were ranked top five in three of the metrics for Toronto 18. Table 4 shows the Toronto 18 top-five actors in each centrality metric, and the top-ranked actors in March 11 are presented in Table 5. Degree centrality counts how many ties each actor has, closeness centrality measures how close on average an actor is to every other actor, eigenvector centrality is similar to degree centrality but takes into account how well connected each actor's neighbors are, and betweenness

centrality measures to what extent an actor is located on the shortest path between all other pairs of actors.

Table 4. Top-Ranked Actors in Toronto 18 by Normalized Centrality Scores.

Degree	Closeness	Eigenvalue	Betweenness
Fahim Ahmad (.722)	Fahim Ahmad (.783)	Zakaria Amara (.482)	Fahim Ahmad (.25)
Amin Mohamed Durrani (.667)	Amin Mohamed Durrani (.75)	Fahim Ahmad (.461)	Zakaria Amara (.181)
Zakaria Amara (.667)	Zakaria Amara (.82)	Amin Mohamed Durrani (.453)	Amin Mohamed Durrani (.17)
Saad Khalid (.5)	Saad Khalid (.621)	Saad Khalid (.433)	Mubin Shaikh (.111)
Ahmad Mustafa Ghany (.5)	Ahmad Mustafa Ghany (.621)	Ahmad Mustafa Ghany (.433)	Jahmaal James (.111)

(After French, 2013). Normalized centrality metrics calculated in UCINET (scores in parentheses).

Table 5. Top-Ranked Actors in March 11 by Normalized Centrality Scores.

Degree	Closeness	Eigenvalue	Betweenness
Jamal Zougam, 1 (.406)	Jamal Zougam, 1 (.639)	Jamal Zougam, 1 (.496)	Jamal Zougam, 1 (.165)
Mohamed Chaoui, 3 (.377)	Mohamed Chaoui, 3 (.622)	Mohamed Chaoui, 3 (.477)	Semaan Gaby Eid, 63 (.141)
Imad Eddin Barakat, 7 (.29)	Imad Eddin Barakat, 7 (.554)	Said Berrak, 41 (.368)	Mohamed Chaoui, 3 (.13)
Said Berrak, 41 (.261)	Said Berrak, 41 (.551)	Imad Eddin Barakat, 7 (.336)	Imad Eddin Barakat, 7 (.11)
Amer Azizi, 11 (.246)	Amer Azizi, 11 (.522)	Amer Azizi, 11 (.335)	Naima Oulad Akcha, 24 (.092)

(After Rodriguez, 2005). Normalized centrality metrics calculated in UCINET (scores in parentheses). The number after each name is the label used in network diagrams.

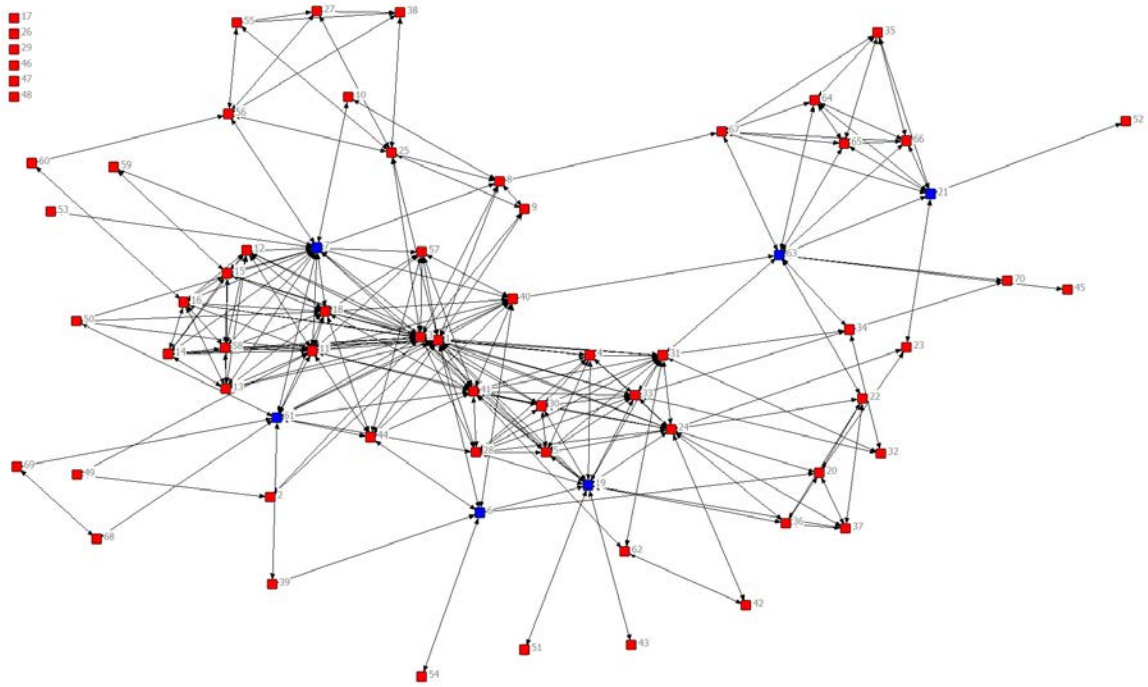
Central actors can be interesting in a targeting perspective, to degrade network performance. Other factors need to be taken into consideration, but actor centrality often provides valuable insight. It is contested whether the most central actors in networks are their leaders, because central actors may be the most vulnerable (Oliver, 2014). Some networks protect their leaders by not putting them in central roles for communication or flow of resources, but removal of central actors is still likely to degrade performance of a network, at least in the short run.

b. Brokers and Bridges

The structural location of actors can be crucial to the flow of information or resources in a network (Everton, 2012). A tie that connects two components that would otherwise be disconnected is called a bridge. The actors on each side of a bridge are called brokers, cut-points, or boundary spanners. If a cut-point or a bridge is removed, the network becomes disconnected. There are only two cut-points in Toronto 18 (Jahmaal James and Mubin Shaikh), and removal of any of them only causes one actor to be disconnected. In March 11, there are six cut-points, indicated in blue in Figure 14. Cut-point analysis is often limited in the case of well-connected networks, where the removal of one single actor may not have a great impact (Everton, 2012). Instead, Borgatti's Key Player program, which comes with UCINET, can be used to identify a set of key players for removal. The program also reveals to what degree the network would be fragmented if the suggested key players were removed. Besides identifying the earlier mentioned cut-points in Toronto 18, the program suggested that the network would be most fragmented if the following three actors were removed: Fahim Ahmad, Amin Mohamed Durrani, and Zakaria Amara. UCINET also has a fragmentation function that indicates the fragmentation resulting from removal of each actor. Values should be compared between each other to see which actor's removal would fragment the network the most. The five actors whose individual removal would fragment Toronto 18 most are the two cut-points and the three actors identified by the Key Player program, which supports previous results. In the March 11 case, the fragmentation mainly increases steadily with the number of removed actors. If only a few actors can be selected, removal of Jamal

Zougam (1), Abderrahim Zbakh (19), and Rabel Osman (61) would fragment the network most. They are all identified in the previous cut-point analysis.

Figure 14. Cut-points in March 11.



(After Rodriguez, 2005). Cut-points are indicated in blue.

c. Constraint

Burt (1992) proposed an approach, built on Marc Granovetter's work in 1973 on weak ties, to measure constraint of actors. The approach focuses on finding gaps in the social structure (which Burt refers to as *structural holes*) that a tie bridges. A structural hole is defined as "a relationship of nonredundancy between two actors" (Burt, 1992, p. 65), and is a way to describe how social structure creates opportunities for some actors. Structural position varies between actors, where "certain players are connected to certain others, trusting certain others, obligated to support certain others, depending on exchange with certain others" (Burt, 1992, p. 57). In an ideal situation, actors can choose freely between alternative relationships, but social structure limits these opportunities and puts constraints on actors (Burt, 1992). The less constraint an actor has, the higher is the

autonomy and possibility to broker information. By calculating constraint on both networks, actors who are important in the information diffusion process can be identified. The five individuals with the lowest constraint in Toronto 18 were Fahmin Ahmad, Zakaria Amara, Amin Mohamed Durrani, Saad Khalid, and Qayyum Abdul Jamal. In March 11 they were Jamal Zougam (1), Mohamed Chaoui (3), Imad Eddin Barakat (7), Abderrahim Zbakh (19), and Said Berrak (41).

D. THE NETWORK DESIGN APPROACH

Now that SNA has been reviewed on both cases, the cases are examined from a network design perspective. The framework from Chapter II is used to structure information, but analysis is not done in this chapter. Here each of the different elements is described, and in Chapter V it is discussed how effective individual elements were, and how well they functioned together as a whole.

1. March 11

March 11 is the first group to be described using the network design framework. Each element of the framework is addressed, as it relates to the specific circumstances of this case. There are some interesting details that make this case special, including the political situation and the timing of the attacks.

a. General Environment

The eight variables that the U.S. Army uses in its operational planning, abbreviated PMESII-PT (U.S. Army, 2011), are used to ensure that relevant aspects of the general environment are considered.

(1) Political

Politically, it was a sensitive time in Spain with the attacks occurring only three days before general elections. The sitting government with Spain's Popular Party was under heavy critique by the oppositional Spain's Socialist Party for Spain's participation in the Iraq war; the opposition promised to end the Spanish involvement in Iraq if they would win the elections (Atran, 2010).

(2) Military

The Basque separatist group ETA had terrorized Spain for decades. They targeted tourist destinations around Spain with bombings, but were under heavy pressure following worldwide toughening of counter-terrorism activities after 9/11. Spanish security forces were increasingly successful in stopping ETA attacks, and the March 11 network had to be concerned with the presence of counter-terrorism agencies.

(3) Economic

The world economy was exceptional in 2004, with the highest growth (5%) in a quarter century (Caruana, 2005). Spain was no different, with a booming economy and an expanding workforce, thanks to immigration and more women in the labor force (Caruana, 2005).

(4) Social

Leading up to the social situation, there was a small group of Muslim migrants who fled Syria in the 1980s and settled in Madrid. Some of them were militants who created a support network for jihadi fighters in Bosnia in the 1990s, and created connections to al-Qaeda in Afghanistan and different parts of Europe (Atran, 2010). The group welcomed jihadists returning from Afghanistan, Bosnia, and Chechnya, and was excommunicated from the mainstream Muslim community for preaching violence (Atran, 2010). They were known to Spanish authorities and put under surveillance, which led to the core group being arrested in 2001. Peripheral members avoided capture and became angry about the arrest of their friends. They started a detailed plot in 2003 to avenge the suffering of fellow Muslims (Atran, 2010).

(5) Information

A variety of information technologies were available, including cellphones and the Internet. The flexibility of these systems must be weighed against the risk of surveillance and the digital tracks they leave.

(6) Infrastructure

There were well-functioning transportation and communication systems in Spain. This operational variable did not present any specific challenges for the group; instead it suggested a valuable target.

(7) Physical Environment

Madrid, with a population of 3.2 million, is the third largest city in Europe (The United Nations Statistics Division, 2013). This implies a significant police force, but also a very diverse population to hide within.

(8) Time

The goal of the terrorists was to force Spanish troops out of Iraq by influencing the general elections scheduled for March 14, 2004. People would still be emotionally shaken if the attacks were conducted just a few days before elections, and there would be confusion concerning what had happened.

b. Key Success Factors

The primary key success factor was to remain hidden. Network coordination and governance is needed, with minimal exposure to the authorities. But just staying hidden has no impact. Resources have to be mustered to carry out the mission, so there is a design challenge. On the one hand, effective communications with a high flow of information and the ability to muster resources are desired. On the other hand, exposure should be minimized to avoid capture.

Appropriate timing of the attacks was vital to influence the general elections. During the attack itself, timing is a key success factor, with great impact on the results.

c. Network Purpose and Direction

Remaining members from the Muslim extremist support group wanted “to carry out violent justice and to right perceived wrongs against Muslims” (Atran, 2010, p. 182). Al-Qaeda designated Spain as a target, and wanted to exploit the opportunity presented with upcoming elections (Atran, 2010). These two different espoused goals were

combined to give the network a clear purpose and direction. The long-term goal was to get Spain to withdraw from Iraq.

d. Network Design Elements

Here a closer look is taken at the network's design elements. What were the different components that made up the network, and how well were they designed? People and skills, roles and tasks, work processes, topography and structure, and other processes are discussed in accordance with the network design framework.

(1) People and Skills

There were 13 members who performed the attacks, but the complete network had 70 members according to Rodriguez (2005). Six out of the 70 were Spanish citizens who had an important role in acquiring explosives (Atran, 2010).

The leadership consisted of two individuals with different backgrounds and skills who complemented each other. Serhane Abdelmajid Fakhet (a.k.a. the Tunisian) was an instigator and spiritual guide, and one of the peripheral members in the Muslim extremist support cell who evaded capture (Atran, 2010). He was well educated, passionate about his ideas, and a devoted warden of Islam (Atran, 2010).

Even though the Tunisian and his followers were motivated to perform an attack, they lacked the capabilities to do so. Here is where the other leader Jamal Ahmidan (a.k.a. the Chinaman) comes into the picture. While the Tunisian is referred to as "the dreamer," the Chinaman is referred to as "the doer," since he was very committed and acted without hesitation (Atran, 2010). The Chinaman was involved in organized crime and was previously convicted, and therefore had the connections and knowledge that the group needed (Atran, 2010).

The group discussed helping fellow Muslims abroad, but Rabei Ousmane Sayed Ahmed (a.k.a. the Egyptian) convinced the group to pursuit jihad at home, where they had the material resources to act (Atran, 2010).

Devotion and determination were the most important characteristics among the members. They did not have any particular practical skills useful for terrorist groups (Atran, 2010).

(2) Roles and Tasks

Leadership is important for keeping the network together when relations are minimized to avoid exposure. Leaders need to maintain the collective vision and manage collaborative processes (Anklam, 2007). The two leaders complemented each other by integrating the visions of "the dreamer" with the actions of "the doer."

Providing the explosives was a critical task; Spanish citizens accomplished this by stealing dynamite from mines (Atran, 2010). The group needed bomb expertise, and it exploited the Chinaman's connections to fill this need (Atran, 2010).

There were several logistical challenges. Locations had to be provided for meetings, bomb making, storing equipment, and accommodating members. Three Moroccan members performed this task through their phone shop, which served as a meeting place (Atran, 2010).

(3) Work Processes

Since bombings were the core of the attacks, anything related to bombs is here considered work processes. Everything else that supports and enables is considered other processes. The network executed its direction by leaving backpacks with bombs in train wagons and setting them off using mobile phones. Each rucksack was filled "with ten kilos of dynamite surrounded by shrapnel of nails and screws, and connected to a cell phone-triggered detonator" (Atran, 2010, p. 199). The explosives were acquired by stealing dynamite from mines, as previously mentioned, and bombs were then built using the Chinaman's connections.

(4) Topography and Structure

The network was built on strong ties created before the mission, since members already had personal relations, and trusted each other because they had shared

experiences from training camps and the war in Chechnya (Rodriguez, 2005). After the terrorists travelled to Spain, they relied on weak ties to avoid detection by counter-terrorism agencies.

The network had a dense core with strong ties in the form of a full mesh; see Figure 8 in the SNA section. The strongest relational ties were interaction based (Rodriguez, 2005). The 13 perpetrators were connected through ties to shared nodes based on participation in al-Qaeda. The complete network resembled a scale-free network with some well-connected hubs and some peripheral actors, and the network was centered on a few actors with high centrality.

The structure of the network was fluid with many weak ties providing operational connections within a large network (Rodriguez, 2005). It was a bounded membership network where prior knowledge was a requirement. Most relations were trust-based and built on shared background.

(5) Other Processes

There were a number of processes enabling the work processes of the network. First, network governance and decision-making are discussed. On a higher level, the governance can be described as follows: al-Qaeda named Spain a target, and a local cell carried out the attack (Atran, 2010). Most decision-making was done at the local level, and focus is on the local cell in this thesis. Global al-Qaeda suggested the target and provided training and experience. Local leadership in Spain made the detailed decisions.

The training of most of the members took place in al-Qaeda camps in Pakistan and Afghanistan before the plot was created and the network was formed (Atran, 2010). Planning and reconnaissance were not very extensive processes. The analysis part of this thesis returns to this fact.

The members had only sporadic interactions to consolidate the network (Atran, 2010). Another important process was raising money to fund the mission, and this was accomplished primarily through drug-related business (Atran, 2010).

e. Style and Culture

Network members came from diverse backgrounds but had a shared identity through common core values, and network style culture were derived from existing social capital. The members were committed to the purpose and had shared norms, which kept the network together despite missing formal organization. The culture was strong despite a lack of governance. Interactions in the network were mostly personal, but there were some transactional and knowledge-based interactions as well. The focus was mainly on outcome rather than discovery. Locales were for the most part owned spaces where meetings and bomb making could take place. Three Moroccan members owned a phone shop where personal meetings were held to foster trust-building relations (Atran, 2010).

f. Results

The output of the network was destruction, measured in terms of 191 civilian deaths and more than 1,500 wounded (Rodriguez, 2005). As to outcomes, the attacks led to public anger against the government. The Spanish population seemed to think that the government lied about facts concerning the attacks, and the origins of the terrorists (Atran, 2010). Spain's participation in Iraq was perceived to be the reason for the attacks. All of this resulted in "discredit of the conservative government and party, and an unexpected turn around in the March 14 elections" (Rodriguez, 2005, p. 6), where Spain's Socialist Party won. The social capital of the government was destroyed, and consequently Spain withdrew its troops from Iraq.

2. Toronto 18

Now the network design model is applied to examine the factors that made Toronto 18 unsuccessful in their particular environment. Using the network design framework, the environment, network direction, network design elements, culture, and results are described.

a. General Environment

Again, the general environment is described using the same eight variables, in accordance with U.S. Army operational planning (U.S. Army, 2011).

(1) Political

The Canadian government was allied with the United States in the war on terrorism. As a consequence, Canada was involved in Afghanistan. In 2001, Canadian commandos were actually the first to hit the ground in Afghanistan ("Canadian Military," 2014). Federal elections were held in January 2006 because of a vote of no confidence for the sitting Liberal minority government (Krauss, 2005). The Conservative Party of Canada received the most votes, and formed a new minority government. The new government continued to support the war on terrorism.

(2) Military

Canada had a well-functioning police force, with support from intelligence and counter-terrorism agencies. Awareness had increased after 9/11, and Canadian agencies cooperated with U.S. counterparts.

(3) Economic

The economic situation in Canada was stable, with a steady annual gross domestic product (GDP) growth (The World Bank, 2015). Lower-middle-class to middle-class households dominated the areas where the group lived, and some of their parents had to work hard, but nothing indicates that the group members experienced any poverty growing up (Bramadat & Dawson, 2014).

(4) Social

Five percent of the population in Toronto was Muslim (Silber & Bhatt, 2007, p. 30). The group members felt alienated and congregated around the Islamic centers where they felt accepted (Bramadat & Dawson, 2014). After 9/11, the members experienced discriminatory treatment against Muslims, which further distanced them from Canadian society.

(5) Information

The Internet was an important information channel for the group. They watched jihadist videos that fueled their anger against the Canadian government for participating

in conflicts against Muslims. Extremist propaganda uses moral shock tactics by highlighting conflicts between Islam and the West. Prolonged exposure to such propaganda may cause moral outrage that plays an important part in radicalization (Silber & Bhatt, 2007).

(6) Infrastructure

The infrastructure in Canada was fully functional. Roads and public transportations offered reliable conduits for travel and transportation. The U.S. border was one obstacle where the group had been hindered earlier from smuggling weapons into Canada (Bramadat & Dawson, 2014).

(7) Physical Environment

The group operated in an urban environment. A mainly Christian population surrounded them, and was in some cases skeptical towards Muslims as a consequence of 9/11. This led to a feeling of loneliness and alienation.

(8) Time

Since they did not have any specific time constraints, there was no formalized time schedule. That fact annoyed Amara, the more impatient of the two ringleaders, who started his own splinter group (Teotonio, 2010). The group had been under surveillance since 2002, but in 2005 they started to make concrete plans and had to be stopped.

b. Key Success Factors

It can be hard for Muslims to socially blend into an unwelcoming Western country, especially if they bear attributes that stand out from the majority of the population. If the group was to succeed, they had to remain hidden. A terrorist group does not want to draw attention to itself by being arrested, for example; it needs to avoid exposure, especially considering the high level of awareness of local security services.

Plotting against the country that is supposed to be their new home, the group needed to keep members motivated and involved. If members start to hesitate, the group

may be destabilized, or someone may turn to the police. There has to be a leader and motivator who can keep the collective vision intact.

Huge impact is required to make a stable Western country change national policy. This requires both significant resources and skills. Connections to a support network may increase a terrorist cell's possibility for success considerably.

c. Network Purpose and Direction

The network's high-level goals were to avenge deaths and injuries of Muslims around the world, and to end Canada's involvement in the Afghanistan war (Bramadat & Dawson, 2014). The vision to accomplish a withdrawal from Afghanistan was possibly encouraged by the success of the Madrid bombings described in the previous case.

Values and beliefs were espoused through interactions with like-minded people in the Muslim community, and key influences came from trusted social networks such as friends and family, religious leaders, and the Internet. Members of this network felt alienated from the local society, and their exposure to radical propaganda gave them a religious renewal (Silber & Bhatt, 2007).

The group members were not notably religious to begin with; they came from moderately religious families at best (Bramadat & Dawson, 2014). They were lonely in an unwelcoming, non-Islamic Western country, where the most welcoming place with like-minded people was the mosque. Religion became a way to regain dignity, find a spiritual call, and promote self-esteem (Bramadat & Dawson, 2014). Terrorism researchers have often questioned the religious motives of jihadi terrorists, and pointed at political motives as a stronger factor, hence Toronto 18 was probably driven by a combination of religious, political, and other motives (Bramadat & Dawson, 2014).

d. Network Design Elements

Here it is examined how the network is configured internally by describing the various network design elements.

(1) People and Skills

The network consisted of 23 individuals according to the set boundaries, most of whom were young. The average age of the 10 convicted adults was only 21.8 years (Bramadat & Dawson, 2014, p. 77). Due to their young age, the members had not acquired any significant experiences or skills, but they had high motivation and took their commitment seriously.

Two members had not practiced Islam before joining the group; converts often want to prove their religious conviction, and are therefore more aggressive (Silber & Bhatt, 2007).

One of the two ringleaders, Fahim Ahmad, was very charismatic and acted as the religious leader by inspiring other members with his violent jihadist views (Teotonio, 2010). The other ringleader, Zakaria Amara, was clever and calculating. He believed that Ahmad talked a lot but did nothing; Amara was more of a doer, and grew impatient with Ahmad (Teotonio, 2010). Just like in March 11, the two leaders can be described as one dreamer and one doer.

(2) Roles and Tasks

Fahim Ahmad and Zakaria Amara were the two leaders, and their tasks were to hold the collective vision, manage processes, and inspire the group members (Anklam, 2007). In addition, Ahmad filled the roles of planning, as well as training, testing, and selecting potential recruits, while Amara handled funding and logistics (Bramadat & Dawson, 2014). One role that was not clear was who would actually drive the trucks with explosives. No one expressed the desire to become a martyr (Bramadat & Dawson, 2014).

(3) Work Processes

Toronto 18 prepared a number of plots to reach their goals. The most concrete was to detonate truck bombs outside the Canadian Security Intelligence Service office, the Toronto Stock Exchange, and a military base (Bramadat & Dawson, 2014). These attacks were scheduled for November 2006, but that depended on when explosives could

be acquired (Teotonio, 2010). Another idea was to attack the Parliament and behead the Canadian Prime Minister (Silber & Bhatt, 2007, p. 30). The group did not get very far in the processes before they were arrested, but they had started to acquire guns, detonators, and explosives (Silber & Bhatt, 2007).

(4) Topography and Structure

The group had a disorganized nature and was far from bureaucratic and formal (Bramadat & Dawson, 2014). Members came together because of preexisting social relationships. Many were friends; friendship was the strongest tie that held the group together and was used to recruit new people (Bramadat & Dawson, 2014).

It was a small and well-connected network, as was discussed in the SNA section of this report. The diameter was 4, and the average degree centrality was 6.842.

(5) Other Processes

The group arranged training camps where members would train for military maneuvers. Although amateurish, the camps created stronger bonds, including between the two subgroups (Bramadat & Dawson, 2014). One member travelled to Pakistan where he is believed to have received paramilitary training (Silber & Bhatt, 2007).

A lot of information management was conducted via the Internet. The group received inspiration and guidance by watching jihadist videos and participating in discussion forums. Most personal interactions took place at Islamic centers and mosques, but the group was looking for a safe house where they could prepare the attacks (Teotonio, 2010).

In an attempt to get funds, the group reached out to a fraudster who could assist in bank schemes (Teotonio, 2010). The group tried to recruit new members by targeting young people around campuses and sports fields (Silber & Bhatt, 2007). Fahim Ahmad made decisions alone, but Zakaria Amara eventually revolted and took charge of the Mississauga section.

e. Style and Culture

The group was characterized by youthfulness and a disorganized nature, but they had a strong sense of purpose (Bramadat & Dawson, 2014). They shared core values about Muslims suffering around the world and the conviction that retaliation had to be taken against the Canadian government. By distancing themselves from the outside world, and reinforcing each other's violent ideas, a secular mindset was built and self-radicalization occurred (Silber & Bhatt, 2007).

Relations were built on friendship, something members could find among the like-minded in the Islamic community when the Canadian society felt alien. Local mosques were a natural meeting place, and the Mississauga cluster all met after school at the Islamic center; spending more and more time there was a way of avoiding problems at home or in school (Bramadat & Dawson, 2014). Most interactions among the group were person-based, but the Internet was an important part of the world they lived in, where they could connect with other radicals across the world to reinforce their ideas. Fahim Ahmad was particularly careless about surveillance and drew attention to himself by posting information on the Internet and handing out CDs about the oppression of Muslims by the West (Teotonio, 2010).

f. Results

The group ceased to exist after raids by police and security agencies commencing on June 2, 2006. At that point, the group had not managed to conduct any attacks, but they still had an impact on Canadian society.

(1) Output

A simple way to quantify output is 18 arrested members, with 11 following convictions (Silber & Bhatt, 2007). This was the tangible output of the network.

(2) Outcome

The most important outcome was that terrorist attacks were prevented through the disruption of the group. Another outcome was that the Canadian population became

aware of the threat of homegrown terrorists (Bramadat & Dawson, 2014). When the group was first exposed, few believed that they had posed any real threat. But as material from the trials became public, it was clear that these seemingly integrated young men were highly motivated and constituted a genuine threat (Teotonio, 2010).

E. SUMMARY

In this chapter, two historical terror groups were described using two different models. The first case was the March 11, 2004, network that detonated bombs aboard trains in Madrid. In the second case, Toronto 18, a terror group active in Canada between 2005 and 2006 was reviewed. Each case was described using both SNA and a network design approach. SNA measures a network's structure empirically through a collection of theories and models, and network design evaluates which configuration is most efficient in a particular environment.

The descriptions are analyzed in the next chapter, again using both perspectives. Strengths and weaknesses are discussed, as well as factors that explain the results of the two cases. Building on insights from these cases, recommendations are made for using the two approaches together to develop strategies to disrupt terrorist networks.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS

This chapter analyzes the results, discusses the merits of the two approaches used, and offers recommendations for countering terrorism. First each case is reviewed, where strengths and weaknesses are analyzed, and what led to the respective outcomes is discussed. Then key insights from using the two analysis models are presented, including the explanatory value of each, and potential limitations of the models. Lastly, recommendations based on the findings of this research are suggested.

A. CASE 1: THE MARCH 11, 2004, MADRID BOMBINGS

The Madrid train bombings were successful; the terrorists accomplished their goal. But why was the network successful? Answering this question may help identify factors that be influenced to prevent future attacks.

1. Performance

Overall, the network succeeded. They achieved their primary goal: to force Spanish troops out of Iraq. It must be considered a victory for terrorism when it can determine a country's foreign policy. The network made a huge impact with little means, but could have been much more efficient. The output was not as severe as it could have been because of poor execution. With simple changes, the number of casualties could have been considerably higher, and it would have been more difficult to capture network members. From the terrorists' perspective, it might have been beneficial that there were not any more casualties; there is a point at which enough damage is done that the population begins to unite against the terrorists' cause.

Atran (2010) states that the network was incompetent, but they were lucky that Spanish law enforcement and intelligence also were inefficient. A lot of information was available to the authorities, but lack of communication prevented them from putting the pieces together. Drug enforcement agencies were aware of some activities, counter-terrorism agencies knew about jihadists, and the theft of explosives was also under

investigation. But government agencies could not make the connection, which resulted in the largest terrorist attack in a Western country since 9/11.

2. Strengths and Weaknesses

The existence of many weak ties proved to be both a strength and a weakness for March 11 (Rodriguez, 2005). Those connections provided operational ties within a larger network, which allowed them to muster resources. On the downside, the large amount of weak ties was also a weakness that led to the capture of most members once authorities started pursuing them. This was after the network had completed its mission and the goal was reached, and the fact that members were killed or captured later was considered by the group to be an acceptable cost.

The core of the network had strong ties built upon trust through previous relations and personal knowledge. This allowed for a strong identity and shared norms without a need for frequent interactions. It was beneficial to rely on existing strong ties and to minimize interactions within Spain to stay undetected.

Because of the members' diverse backgrounds and lack of specific skills, the network avoided attention. Perhaps this was a fitting configuration since they were successful. If the network had included more competent actors, it would have been more interesting to the authorities. Also, it was not a great concern if some members got killed or captured during or after the attacks, since they did not have any valuable skills.

The Chinaman's connections were valuable for constructing bombs, but one of the bombs did not detonate. With better bomb-making skills, that bomb might also have exploded. Authorities were able to track down members through a recovered phone. The SIM card had been used for phone calls and it also carried fingerprints (Atran, 2010). These were amateurish mistakes illustrating weaknesses in the network.

The attackers relied on time schedules when detonating the bombs. The trains were supposed to be at train stations, which would have led to thousands of victims (Atran, 2010). But the trains were not on time, bombs detonated between train stations, and many potential victims were spared.

3. Configurational Fit and Result

The network evolved from being informal to more formal. It had its roots in spontaneous informal networks that emerged opportunistically around an issue without defined roles or purpose (Atran, 2010). But at the time of the attacks, it had moved towards a formal network with a purpose and goal that directed collective action. The network then had membership requirements, roles, tasks, and processes in place. Processes for decision-making, budgeting, communications, and planning were not well developed, which led to the underutilization of resources and inefficient operations.

The network had traits of both hierarchies and heterarchies. There were individuals with more influence than others, but that was because they were determined and motivated. They did not put themselves above other members; they were only enthusiastic to move the network forward. In a larger perspective, the local cell was very low in the al-Qaeda hierarchy. But that did not bother the members.

The network used shared governance. Of course, global al-Qaeda nominated Spain as a target, but the local members already wanted to strike in Spain. They took shared responsibility for decision-making without central authorization. If the governance had been more central, the network might have been more successful.

If network design elements are not aligned with each other, with the environment, and with network direction, design tensions can develop. The most important factor that suppressed such tensions was the leaders' ability to hold a collective vision and manage collaborative processes (Anklam, 2007), which led to a style and culture well reflecting the group's purpose and direction. Shared norms and core values were strong enough to prevent occasional tensions from disrupting the network.

As mentioned earlier, the network design elements were not all optimal, but they were a good enough fit to reach the objective; more importantly, they were a good fit with the environment. The network remained undetected and achieved its desired outcome. Perhaps the lack of skill and organization were the very success factors that allowed the network to avoid detection by the authorities (Atran, 2010).

B. CASE 2: TORONTO 18

Toronto 18 was completely disrupted by police and security services, and there were several significant differences compared to the March 11 network. In this section, the data described in Chapter IV is interpreted to understand why Toronto 18 failed.

1. Performance

The group performed worse than the police and was disrupted while still in the planning process. It did not get a chance to produce any output in the form of damage or death. If some processes had been managed well, they might have been more successful. Communication, both personal, on the Internet, and on cellphones, should have been much more restrictive. The group made the police's job easy by being ignorant of surveillance. One explanation is that the members were young, which led to youthful enthusiasm without reflection.

2. Strengths and Weaknesses

Determination was their biggest strength. They had a strong sense of purpose and were focused on their task to retaliate against the Canadian government. Another strength was the culture, with solid bonds through shared values and norms. Friendship was very important in the network. This factor contributed to the strong determination of the members, but the need for friendship opened the group up to informants, who used this to gain access to the group.

High density in a network improves the flow of information, but it also makes the group more visible. Since the average path distance between actors was only 1.860, information spread to most members quickly. On the other hand, this meant that informants would likely have access to a lot of information as soon as they joined the network. Informants may not have had the same access to information if the network had been less dense.

Group members had no relevant skills about terrorism or criminality: Mohammed Ali Dirie had a prior conviction for smuggling firearms from the United States, but he was the only member with a significant criminal record (Bramadat & Dawson, 2014).

The group tried to acquire knowledge via the Internet, but their behavior was youthful and amateurish. If the group had been more security aware and had kept a lower profile, it would have been more difficult for law enforcement agencies to track them and later convict them. In addition, if it had had been more careful screening recruits and members, the two informants might have been less successful.

3. Configurational Fit and Result

There seemed to be a culture of invincibility, as if the network somehow was protected by serving higher goals. This increased the visibility and vulnerability of the network, as attention was not directed towards network design, specific skills, or external factors.

Considering the environment, the network needed a stealthier configuration. The police were aware of the terrorist threat, and the group should have focused more on staying hidden. They could have made the network less dense by minimizing connections, both personal and electronic. Communicating less often, using different places for meetings, and not discussing as openly would have been more suitable in that environment. If they did not express their beliefs as loudly, they might have received less attention from the police. On the other hand, extensive communication and strong beliefs were the foundations of the group. Without that strong culture, the group might have been destabilized.

The structure was informal and disorganized with a small size and many ties. If they had been more centralized, they would have had more control. That might have been a better fit considering the environment and the existing people and skills.

Since the group was well connected, there were no clear cohesive subgroups identified from social network analysis (SNA). Also there were no real key nodes with bridging properties. The group was separated into two geographical locations, which would have been clear if geographical data had been included in the analysis. In addition, the links that connected the network were recorded over a period of time. Perhaps the network diagram in Figure 10 is not an accurate picture because the group was splitting

in two. Here, dynamic network analysis might have helped to identify changes in the configuration.

Taking into account that the group was well connected, the police applied the correct strategy in conducting several simultaneous arrests. This efficiently disrupted the network, with no chance of recovery. Therefore, the group was unsuccessful, no attacks were performed, and 11 members were convicted.

C. DISCUSSION

This section presents a summary of what can be learned from the two case studies. Insights from using the two models, merits of both models, and potential problems with the models are discussed.

1. Key Insights

Spanish agencies did not communicate well with one another, despite the lessons identified by the reporting and awareness failures leading up to 9/11. They were not able to connect the dots between drugs, explosives, and jihadists, even though all three subjects were under investigation in different departments (Atran, 2010). It is essential in counter-terrorism to keep track of information already available, and to communicate among different departments and organizations. The United States, for example, learned its lesson after 9/11 and has taken several steps to improve efficiency in government inter-organizational work. In the first case study, the terrorists constructed a better-designed network than the Spanish security services. In the second case, the well-designed Canadian counter-terrorism network out-designed the terrorist network. A well-designed counter-terrorism network with good communication has a better chance of defeating a terrorist threat.

Rodriguez (2005) concludes that terrorist groups, unlike conventional military units, “often use dispersed forms of organization, which can balance the need for covertness with the need for broader operational support and resources” (Rodriguez, 2005, p. 23). Similarly, Everton (2012) suggests that the optimal levels of centralization and density depend on the environment. Dark networks need some level of bureaucracy

to be efficient. It is a fine line between not being able to muster resources, and being too visible to the authorities. Also, it is a challenge to balance "the need for access to network members (in order to enact leadership or control) and the need to protect leaders by reducing visibility" (Oliver, 2014, p. 15). Toronto 18 was more visible than the March 11 network, which exposed the group to the authorities. A key success factor for any dark network is to stay hidden, and the March 11 network found a suitable configuration while Toronto 18 did not.

Since Toronto 18 was a well-connected network, it could not be disconnected by the removal of only a few actors. To successfully fragment the network, a large number of actors had to be removed at the same time, and this is what the police did through a series of coordinated arrests. The March 11 network, on the other hand, had more cut-points; here the removal of only a few key actors would fragment the network significantly. Individual skill may also influence network properties such as density because well-educated actors may consciously minimize communications (Oliver, 2014).

The small size and the short average path distance of Toronto 18 made information easily available throughout the network. This fact made the group suitable for inserting informants into the network, since they would be close to a lot of information wherever they were connected. French (2013) also identified this fact, noting that the small, tight group was susceptible to informants, and that the informants were placed well to access a lot of intelligence. The March 11 network was less susceptible to informants since they used less communication, built on previous relations, and had stricter requirements for membership.

The networks showed some important differences that contributed to the different levels of success. March 11 had a larger support network, from which they could draw resources and knowledge. A lot of these ties were forged during participation in wars or training camps, where the March 11 members acquired higher skills than the members of Toronto 18. In addition, communication was more covert and infrequent in March 11, which made the network less visible to the authorities than Toronto 18.

Lessons identified about one dark network cannot be directly transferred to another network, because network purpose and direction, environment, and other endogenous and exogenous factors affect network structure (Oliver, 2014). Therefore, SNA metrics cannot be directly compared between cases without considering other factors, endogenous and exogenous.

Studying the environment can identify key success factors in a particular situation. Although some environmental differences exist between the two cases, many variables are similar, and have similarities to the environment in other Western countries. This is the environment of interest throughout the thesis, and a few generic key success factors can be identified. It is essential for the dark network to stay hidden. But they still need connections to a support network to be successful. Also they need to recruit members who are motivated, skilled, trustworthy, and who preferably can blend in among the population.

There were built-in design tensions in both cases, where particular elements were not well designed, or were not aligned with the environment or direction. But the groups did not care about this; obviously they did not pay enough attention to design their networks for optimal performance. One reason may be that they were ideologically motivated and felt that they served a higher purpose, which somehow would protect them. Ideologically motivated groups may develop an insular culture, where too much focus is directed inwards, and the outside world is ignored.

2. Merits of the Two Approaches

SNA is a collection of theories and methods to empirically measure a network's structure, while network design is a theory for determining which configuration is most efficient in a particular environment. SNA provides many metrics that can be used to classify a network and to compare different networks. It also offers a lot of metrics to identify actors who have key roles in the network, based on power, prestige, or information. In addition, SNA includes techniques to identify clusters, subgroups, and factions within a network. All these measurements can be used to inform the decision-making process when choosing strategies to disrupt a network. In many cases, SNA

presents predictive metrics of the resulting network if different nodes and ties were removed. This mathematical approach is suitable for computer networks or biological systems but it is very hard to predict what will happen after a node or tie is removed when dealing with human beings. The network design approach is one way to help predict that, through detailed analysis of a network's configuration in a specific environment.

Performance can be explained by studying how a network's design elements are configured to match the environment and each other. The network design approach allows an examination of the network design elements' configurations and their alignment with each other and the environment. It is a sign of a poor configuration if the culture in a network does not match the direction. SNA is assumed to identify vulnerabilities in a network through structural properties, but other exogenous factors need to be considered (Oliver, 2014). Perhaps SNA suggests that the removal of a few actors would fragment a network. But if the network is not performing well, a better option may be to do nothing at all. The existing configuration might be a poor fit for the environment, and government intervention should not improve the fit. If the group concentrates too much on work processes, the performance suffers as other network design elements are neglected. Terrorist networks, like other organizations, depend on good management.

SNA often describes a snapshot in time when ties are recorded and analyzed. Sometimes a dynamic model is needed to explain the formation, evolution, and termination of networks. Dynamic network analysis is one way to approach this, but several exogenous and endogenous factors may be neglected, and that is where the comprehensive network design perspective is valuable.

The network design approach can also be used when no empirical data are available. By analyzing an environment, it is possible to identify the key success factors in that situation. Then, security services should look for signs that someone is trying to pursue these factors. It can be a particular skill or a special component, which is crucial.

It is possible that the network design approach is less vulnerable to errors than SNA. SNA is sometimes unconditional; if there is no tie between two actors in a network diagram, it seems as if they are not related at all. That is not necessarily true; the actors can be related through a type of relation not collected and analyzed. Perhaps the time of the snapshot is not representative to describe network structure, or the network has already evolved and changed since data were collected; longitudinal network analysis attempts to attack this problem. Data can also simply be missing or erroneous; one missing link may significantly change the network structure and various metrics. The network design approach is more general than SNA; while it does not offer as specific output as SNA, the network design approach is not as sensitive to errors. The idea is to look at the big picture and identify weaknesses and strengths in a network to be able to exploit them. Another benefit from the network design approach is that it may help explain results derived from SNA, for example, why network centralization has changed over time. Factors that may cause different SNA metrics include changes in environment, leadership, or network direction. Applying the network design approach to analyze dark networks may provide a context in which strategies proposed from SNA can be validated. It is definitely another tool in the toolbox to inform counter-terrorism decisions.

3. Potential Problems

As in all research, the quality of the available data determines the accuracy of the analysis. Having incomplete data is a common problem when analyzing dark networks, and data can also be biased when media or governments publish it. This issue is quite relevant for both analysis models used in this thesis. Information has to be valued and preferably confirmed by two independent reliable sources. That is not always possible, of course. If high quality data can be accessed, the possibility for developing efficient strategies increases.

D. RECOMMENDATIONS

Recommendations based on the research results are presented in this section. The recommendations are expressed at several different layers, spanning from the organization of government agencies to the application of specific analytic tools.

1. General Guidelines

It is preferable to intervene as early as possible in the network development process to efficiently disrupt a terrorist cell. If the formation of a group can be blocked, fewer network members must be targeted to prevent recovery. It is possible to do more damage to the terrorist network by identifying and targeting individuals with wider skillsets. These individuals serve as facilitators, or "network engineers." They set up a network, get it going, and then assume a more withdrawn role. This is the weak link in the network formation process and a definite high payoff target.

Another approach is to target unique skillsets or components that are crucial to the terrorist network. If a single vital component or skill can be disrupted, it may halt the whole mission. What this component is depends on the environment. Certain components are very hard to acquire in some situations. Each environment must be analyzed to identify what these components may be. Countries should analyze their own environments to identify what terrorists need in order to be successful there. Then they should focus their efforts on denying terrorists access to that component; e.g., if explosives are available to terrorists, but detonators are hard to get, focus on denying them access to detonators. Or if bomb-making skills is the most valuable component, focus on identifying and monitoring anyone with such skills.

According to the network design framework, what parts of the network should be addressed? Can direction of terrorist networks be changed? That may be possible through political adjustments and dialogue with extremist organizations. The treatment of returning fighters is one important issue that countries must deal with. Furthermore, the environment could be changed, but is that desirable—that is, should surveillance of the public be increased, and people's rights limited? That may be as frightening as terrorist attacks. The ambition should be to increase the efficiency of counter-terrorism agencies. Terrorists need to be out-designed, so that government organizations are more efficient than terrorist networks. Law enforcement agencies cannot configure the terror cells, but from this analysis, more is known more about how they have been configured, and what to look for.

2. What to Look For

One important question is how jihadi networks are created? Sageman (2004) concluded that recruitment to the global jihad comes primarily through pre-existing social ties. In his study, 75% of the global jihad members joined through pre-existing kinship and friendship ties. Bakker (2006) found in his study of 242 jihadi terrorist and 28 terrorist networks that even though the networks differed in size, scope, and success rate, they were all internally homogeneous. The networks "tend to form around people who share age group, country of family origins, and the country in which they live" (Bakker, 2006, p. 34). This implies the need to monitor individuals with known ties to terrorist-related organizations. They may recruit new members, so these individuals constitute an important starting point in the search for potential terrorists.

Sleeper terrorist cells may have ties to the supporting organization, whether it is al-Qaeda, ISIS, or some other. There may be an exchange of resources or information that can be detected. Therefore, it is valuable to have access to conversations, travel records, and other data to recognize the threat before it is too late.

Special attention should be paid to popular terrorist targets, such as large cities, special events, and other places where a lot of people gather, and where media coverage is present. These are places where terrorists may have high output, regarding both causalities and attention.

Public support is needed for extensive monitoring; the public usually opposes government surveillance if they cannot see the need for it. Sometimes the need is not apparent until after an attack. In the wake of 9/11, citizens in the United States and other countries afraid of terrorist attacks accepted a significant increase of video surveillance (Linn, 2011). The Security Service in Sweden was not allowed to task the national signal intelligence because of public concerns about privacy, but after a failed suicide bombing in downtown Stockholm on December 11, 2010, voices were raised to allow the Security Service that possibility (Hansson & Holmström, 2011). It is vital that the public understands why surveillance is important, and that they recognize the terrorist threat. Of course there have to be clear directions regarding the use of surveillance and the

collection of surveillance data. But public support increases if the need for surveillance is accepted.

3. Organizational Policies

Milward and Provan (2006) describe what McChrystal realized: "It takes a [decentralized] network to defeat a [decentralized] network" (McChrystal, 2011, p. 69).

> Government leaders are increasingly finding that using traditional hierarchical organizations does not allow them to successfully address complex problems, such as homeland security, emergency response to disasters, and the delivery of social services. As a result, they are beginning to explore the use of collaborative networks that reach across agencies and programs. (Milward & Provan, 2006, p. 4)

As learned from 9/11 and the 2004 Madrid bombings, coordination between different security agencies is crucial. Information diffuses much faster in a dense and decentralized network (Borgatti et al., 2013), which is one key to success. Countries need to organize different agencies as a network of networks (Anklam, 2007), where each organization is structured like an informal, decentralized network, and where the organizations all collaborate in an informal, decentralized way. Milward and Provan (2006) argue that decentralized networks "are the only organizational forms that can operate horizontally, across a range of organizations, and integrate the strengths and talents of a variety of organizations in the public, nonprofit, and for-profit sectors to effectively address critical public problems" (Milward & Provan, 2006, p. 7). There are several challenges with building such a network successfully. A good start is to create informal relations to build trust. Personal interactions are recommended initially to build trust quickly, but then appropriate communication systems have to be in place so that individuals in different locations can quickly and easily share information with each other. The focus should be on expertise, and not on titles or rank. There has to be a shared goal and a culture that is aligned with that goal. Design matters, and terrorist networks have to be out-designed by making counter-terrorism agencies more efficient.

If laws or policies limit agencies' abilities to share information, performance may decrease, and the threat may increase. U.S. law was changed after 9/11 as the Patriot Act

overruled some limitations set in the earlier Privacy Act. Government's right to monitor citizens is an important question and should not be accepted easily. There has to be discussion and debate about which is worse for a democracy: government surveillance or terrorist attacks.

4. Dynamic Network Analysis

Dynamic network analysis involves observing changes in networks, often over time. Terrorist networks have repeatedly rebuilt themselves extremely well after attempts to disrupt their organizations; therefore, longitudinal analysis is very interesting (Rodriguez, 2005). By studying data over time, changes can be detected, analyzed, and explained.

Social network change detection (SNCD) is a method for real-time analysis of a network to detect sudden changes. When a change is detected, attention can be focused on explaining the cause of change. As suggested by McCulloh and Carley, "terrorist organizations will begin planning their attacks, long before they are actually carried out. Rapid change detection could alert military intelligence analysts to the shift in planning activities prior to the attack occurring" (McCulloh & Carley, 2011, p. 5). One problem with this technique is determining what constitutes a significant change. A too-low level results in false positives, and a too-high level misses significant changes. This method should nonetheless be considered if longitudinal data are available.

5. Taking a Positional Approach

As described in Chapter II, one method in SNA is to focus on the position of actors in social structures. Actors in similar positions may exhibit similar behavior. Therefore, individuals in positions likely to engage in jihadist activities should be identified. First a role "Fighting for ISIS" is defined. By examining the ego networks of known individuals in this role, those individuals' structural positions can be specified. Since individuals in similar positions are believed to exhibit similar types of behavior (Everton, 2012), individuals in similar positions should be searched for to identify potential recruits, and then prevented from joining ISIS.

Individuals closely tied to a network's leader are less likely to defect, and time should not be wasted on trying to reintegrate them (Everton, 2012). Actors in a block close to the network leader should instead be closely tracked since new leaders are likely to emerge from this cluster (Everton, 2012). They should be targeted with a harder approach such as arrest, because the network may be disrupted and fragmented if these central actors are removed. Softer approaches may be more suitable for peripheral potential recruits. Then the government should try to reintegrate them and prevent further radicalization. In this way, a combination of hard and soft approaches may have the best effect on disrupting terrorist networks.

6. Strategies to Disrupt Dark Networks

Exploration of a dark network's topography is an important input in order to develop effective disruption strategies, kinetic or non-kinetic. The provincial–cosmopolitan and hierarchical–heterarchical dimensions can reveal a lot about which category of actors to target, which strategies are suitable, and how the network will react. The first dimension describes whether the network is provincial (sparse) or cosmopolitan (dense), and the second whether the network is hierarchical (centralized) or heterarchical (decentralized). A dark network is believed to be most efficient if it has a balance between the two extremes in both dimensions (Everton, 2012; Rodriguez 2005). If the topological analysis shows that a dark network is balanced in these dimensions, strategies are needed to change that. But if the network is not balanced, nothing should be done that may make it more efficient. For example, if a dark network is too dense to be efficient, removal of hubs may possibly make the network more efficient. Instead, peripheral actors should be targeted to make the network even denser and more inefficient. A kinetic strategy can be applied such as capturing actors, or a non-kinetic such as enticing them to leave.

Well-configured terrorist networks post the greatest challenge, where no clear design tensions provide vulnerabilities to be exploited. The networks have to be studied carefully in search of a weakness, perhaps a unique skillset or resource. Here designing

counter-terrorism agencies to be more efficient is particularly important; the terrorist networks are battled in a design contest.

A highly centralized network is more vulnerable to the removal of key actors (Everton, 2012), so if a dark network is highly centralized, it is best to try to remove central actors. Centralized dark networks are less resilient than decentralized ones (Bakker, Raab, & Milward, 2011). A network may be shaped into a more vulnerable form through initial non-kinetic strategies, and then kinetic attacks can be applied.

Another important merit of SNA is the identification of individuals at risk of being recruited. Once these individuals are identified, preventive measures can be applied to stop them from joining or to recruit them as informants. Also, members with motives different from the group's purpose and direction should be targeted; they may be easier to convert. If personal motives are aligned with the network's general direction, the network is more likely to be successful.

If a kinetic strategy to disrupt a network is planned, it should be combined with a non-kinetic approach (Everton, 2012; Roberts & Everton, 2011; Tilly, 2005). If some actors are removed, it is important to prevent others from simply replacing them. This can be done through information operations, psychological operations, or rehabilitation and reintegration programs (Everton, 2012).

SNA can be used to suggest both kinetic and non-kinetic strategies. Vulnerabilities in the network can be identified, such as brokers, bridges, or structural holes. Central actors can be targeted either by kinetic approaches such as removal, or by non-kinetic approaches to influence them. In a well-connected network like Toronto 18, several hubs have to be removed at the same time, just as the police did in that case, or it may remain operational. Rodriguez (2005) identified key actors in his analysis of the March 11 network and suggested that removal of a few nodes and links might be enough to destabilize the network. He proposed the removal of nodes with bridging roles, and central nodes in each cluster. Only kinetic approaches were proposed, but non-kinetic approaches should be integrated. Peripheral nodes may be easier to reintegrate or recruit when leaders are gone.

The goal of the strategies is to disrupt or destabilize the network. But what does that mean? The following is a good definition of destabilization:

> There are at least three indicators of destabilization. One is where the rate of information flow through the network has been seriously reduced, possibly to zero. A second is that the network, as a decision-making body, can no longer reach consensus, or takes much longer to do so. A third is that the network, as an organization, is less effective; e.g., its accuracy at doing tasks or interpreting information has been impaired. (Carley et al., 2002, p. 84)

Hopefully this discussion has led to some insights that may contribute to strategies to disrupt terrorist network. The two analysis models used may be valuable assets in the collection of tools to inform the decision-making process.

E. SUMMARY

Both cases have been analyzed through a review of strengths and weaknesses, and what affected their performance. The March 11 network had a more suitable configuration than Toronto 18, and that is why they were successful. Considering the environment, the March 11 network had a more appropriate structure, and they also had better-performing network design elements.

One key insight is that law enforcement agencies have to keep track of available information and communicate well externally and internally. Furthermore, it is suggested that a balanced configuration is required for terrorist networks to perform well; they need to stay hidden, but also be able to muster resources.

Merits of the two approaches have been discussed, along with the potential problems of using them. The chapter concluded with generic recommendations on several different layers.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Western countries fear terrorist attacks that are a result of the ongoing war on terrorism. Terrorist organizations such as al-Qaeda and ISIS have facilitated several devastating attacks in the last decades, and recent events show that the threat is still real. Efficient strategies must be available for government agencies to disrupt these networks and to prevent future attacks. A thorough understanding of networks is required to develop and select the most appropriate strategies. Social network analysis (SNA) is one relational approach for measuring network structure based on empirical data, and it can be used to develop strategies to disrupt dark networks. This thesis examined how a network design approach can be used together with SNA to understand how terrorist networks function, and what made historical cases successful or not. The network design approach is a theory for determining which configuration is most efficient in a particular environment. A case study of two historical terrorist attacks in Western countries was conducted in search of knowledge that can help prevent future attacks through efficient counter-terrorism strategies. The unit of analysis was local terrorist cells that perform the attacks, and not global terrorist networks.

The 2004 Madrid train bombings was the first case of study. This case is important because the terrorists were able to force Spanish troops out of Iraq as a consequence of the attacks. Next Toronto 18 was examined, a Canadian terror group active between 2005 and 2006. That terror group was completely disrupted through a series of coordinated police and security service operations, and the reasons why the group was disrupted provide a good example of successful counter-terrorism efforts. There is a lot of information publically available in both cases, and data were collected from historical records. The significance of the cases, along with the quality of available information, ensured that reliable data were used in the study.

Both cases were analyzed using SNA and a network design approach. The SNA portion was largely based on previous research; this thesis aims to show how the network design approach adds value in network analysis. Network structure and configuration was explored using the different analysis approaches to describe how the terrorist networks

functioned. SNA provides several metrics to describe network topology, and to identify important actors. These metrics can be used to craft strategies that would disrupt the networks. The network design approach takes another perspective in looking at the different internal network design elements and how well they are aligned with each other and with the environment. More network factors are considered than in SNA, including how they fit together as a whole. A network culture that is not coherent with espoused values and beliefs indicates that there are design tensions in the network. This thesis has demonstrated how the two methods can be used together to provide knowledge to inform the process of developing and selecting strategies to disrupt dark networks.

The network design approach can be used to verify results of SNA and to explain differences in SNA metrics over time. It may be less sensitive to errors but does not give as specific results. Through the study, it was shown that both approaches can be used to identify strengths and weaknesses in networks. Strengths and weaknesses vary between different situations; the environment of interest in this thesis has been a Western country, and by learning from previous events, future attacks in similar environments may be prevented. One key success factor for terrorist networks is balancing the need to stay hidden with the need for resources and operational support, and they are most successful when a balanced configuration in terms of density and centralization is reached. Strategies to disrupt terrorist networks should aim to remove this balance, not improve it; therefore, it is important to understand how the network structure is aligned with the environment before choosing strategies. The Madrid network was better configured for its environment than Toronto 18; that is what caused the different outcomes.

The case study led to a number of general recommendations for counter-terrorism. Besides analyzing how terrorist networks are designed, the design of *counter-terrorism* networks must also be taken into consideration. It is important for government agencies to collaborate; information has to be communicated and made available to the ones who need it. Information diffuses faster and decisions are more likely to be correct and timely when decentralized, informal networks are implemented. Terrorist networks have to be out-designed by effective counter-terrorism networks; this is an ongoing contest that must be given the appropriate attention.

A specific component or skill may be identified when analyzing what is needed in a certain environment to be successful. This key resource will vary between situations, but when identified, the resource should be denied the adversary to prevent its ability to conduct operations.

A positional approach can be taken in SNA to identify individuals likely to get recruited by terrorist networks, and they should be prevented from joining. Another interesting branch of SNA is dynamic network analysis, where data are studied over time to detect changes in networks. If a sudden change is detected, it can be an indication that something significant has changed in the network, for example, an attack is imminent (McCulloh & Carley, 2011).

If a kinetic strategy is selected to disrupt a dark network, it should be combined with non-kinetic strategies (Everton, 2012; Roberts & Everton, 2011; Tilly, 2005). The network may be more susceptible to non-kinetic strategies after key actors are removed; i.e., it may be easier to reintegrate peripheral members when they are under less influence of strong leaders. The network is more likely to recuperate through other actors taking the places of the removed ones if no non-kinetic strategies are applied after a kinetic one. Non-kinetic strategies can also be used to shape the network into a form that is more vulnerable to kinetic strategies. In conclusion, the two variants should be used together.

One significant current issue is how to handle citizens who return to their home countries after fighting with ISIS or other extremist organizations. There is a concern that they support terrorist networks with recruitment, for example. Studies show that recruitment to terrorist organizations is largely done through pre-existing relations (Sageman, 2004; Bakker, 2006). Individuals with known ties to terrorist organizations should be monitored closely, and proactive measures should be taken to stop them from expanding the jihad movement. Government monitoring of citizens is a delicate question, and public support is needed for such intrusions of privacy.

Follow-up research should be done on how to best handle returning fighters. Some countries try hard approaches, others soft. It remains to be proven which approach is more successful; maybe a combination of the two is possible. This thesis has only been

concerned with local terrorist cells already planning a specific attack. Global terrorist networks must be battled on a larger scale by targeting recruitment and countering their motives, which was beyond the scope of this thesis.

Another interesting follow-on study would be researching the design of the law enforcement networks for each case. The terrorists won the design contest in Spain, but lost in Canada. Clearly, the government agencies involved in these cases had various levels of success, and a detailed analysis of the factors influencing the agencies' performances may provide valuable directions for counter-terrorism organizations.

The analysis in this thesis has only used publically available information. A more accurate analysis can be made if detailed, possibly classified, data are available. Further cases need to be analyzed before a definitive statement can be made on the usefulness of a method that combines SNA and network design. This thesis has demonstrated that the two methods have merit and that they can be useful tools when designing strategies to disrupt terrorist networks.

LIST OF REFERENCES

Anklam, P. (2007). *Net work: A practical guide to creating and sustaining networks at work and in the world*. Amsterdam, The Netherlands: Elsevier/Butterworth-Heinemann.

Arquilla, J. (2009). *Aspects of netwar and the conflict with al Qaeda*. Monterey, CA: Information Operations Center.

Arquilla, J., & Ronfeldt, D. F. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: Rand Corporation.

Astier, H. (2015). Charlie Hebdo attack: French values challenged in schools. *BBC*. Retrieved from http://www.bbc.com/

Atran, S. (2010). *Talking to the enemy: Faith, brotherhood, and the (un)making of terrorists* (1st ed.). New York, NY: Ecco Press.

Bakker, E. (2006). *Jihadi terrorists in Europe*. Clingendael, The Netherlands: Netherlands Institute of International Relations.

Bakker, R. M., Raab, J., & Milward, H. B. (2011). A preliminary theory of dark network resilience. *Journal of Policy Analysis and Management, 31*(1), 33–62.

Barabasi, A., & Bonabeau, E. (2003). Scale-free networks. *Scientific American 288*(5), 60–69.

Belgium deploys troops following anti-terror raids. (2015, January 17). *BBC*. Retrieved from http://www.bbc.com/

Berman, E. (2009). *Radical, religious, and violent: The new economics of terrorism*. Cambridge, MA: MIT Press.

Blanchard, B. S. (2008). *System engineering management* (4th ed.). Hoboken, NJ: Wiley.

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2013). *Analyzing social networks*. Thousand Oaks, CA: Sage.

Bramadat, P., & Dawson, L. L. (2014). *Religious radicalization and securitization in Canada and beyond*. Toronto, ON, Canada: University of Toronto Press.

Burt, R. S. (1992). *Structural holes: The social structure of competition*. Cambridge, MA: Harvard University Press.

Bye Skille, O., Strand, T., & Alayoubi, M. (2014, November 16). Avhopper til NRK: – IS har sovende celler i Europa. *NRK*. Retrieved from http://www.nrk.no/

Byman, D., & Williams, J. (2015, March–April). ISIS vs. al Qaeda: Jihadism's global civil war. *The National Interest*. Retrieved from http://www.nationalinterest.org/

Canadian military involvement in Afghanistan formally ends. (2014, March 12). *The Canadian Press*. Retrieved from http://www.cbc.ca/

Carley, K. M., Lee, J., & Krackhardt, D. (2002). Destabilizing networks. *Connections, 24*(3), 79–82.

Carling, M. (2015, January 17). Örebros plan för hemvändande jihadister möter kritik. *SVD*. Retrieved from http://www.svd.se/

Carrington, P. J., Scott, J., & Wasserman, S. (2005). *Models and methods in social network analysis*. Cambridge, United Kingdom: Cambridge University Press.

Caruana, J. (2005, June 10). *Overview of the Spanish economy in 2004*. Madrid, Spain: The Governing Council of the Bank of Spain.

The Commission on Presidential Debates. (2008, October 7). The second McCain–Obama presidential debate [Debate transcript]. Retrieved from http://www.debates.org/

Cordoba, J. R. (2006). Using Foucault to analyze ethics in the practice of problem structuring methods. *Journal of the Operational Research Society, 57*(9), 1027–1034.

Cronin, A. K. (2009). *How terrorism ends: Understanding the decline and demise of terrorist campaigns*. Princeton, NJ: Princeton University Press.

Cruickshank, P., Castillo, M., & Shoichet, C. E. (2015, January 15). Belgian operation thwarted "major terrorist attacks," kills 2 suspects. *CNN*. Retrieved from http://www.cnn.com/

Dahl, V. (2014). *Breaking the law: Adolescents' involvement in illegal political activity* (Doctoral dissertation). Örebro, Sweden: Örebro University.

Denning, D. E. (2011). *Axioms of social networks*. Unpublished manuscript, Naval Postgraduate School, Monterey, CA.

de Nooy, W., Mrvar, A., & Batagelj, V. (2005). *Exploratory social network analysis with Pajek*. New York, NY: Cambridge University Press.

Emery, N., Earl, R., & Buettner, R. (2004). Terrorist use of information operations, *Journal of Information Warfare, 3*(2), 34–45.

Emirbayer, M., & Goodwin, J. (1994). Network analysis, culture, and the problem of agency. *American Journal of Sociology, 99*(6), 1411–1454.

Europol. (2014). *European Union terrorism situation and trend report 2014* (TE-SAT 2014). The Hague, The Netherlands: European Police Office.

Everton, S. F. (2012). *Disrupting dark networks.* New York, NY: Cambridge University Press.

Everton, S., & Cunningham, D. (2011). *Terrorist network adaptation to a changing environment*. Unpublished manuscript, Naval Postgraduate School, Monterey, CA.

Faiola, A., & Mekhennet, S. (2014, October 19). Denmark tries a soft-handed approach to returned Islamist fighters. *Washington Post*. Retrieved from http://www.washingtonpost.com/

French, N. N. (2013, March). *Project report: Toronto 18 terror group.* Unpublished manuscript, CORE Lab, Naval Postgraduate School, Monterey, CA.

Garcia-Abadillo, C. (2004). *11-M, la venganza*. Madrid, Spain: La Esfera de los Libros.

Granovetter, M. S. (1973). The strength of weak ties. *The American Journal of Society, 78*(6), 1360–1380.

Hansson, M. E., & Holmström, M. (2011, December 7). FRA-lagen i vägen för jakten på terrorister. *Svenska Dagbladet*. Retrieved from http://www.svd.se/

Ignatius, D. (2014, October 21). A small organization offers a fresh approach on preventing terrorism. *The Washington Post*. Retrieved from http://www.washingtonpost.com/

Italy investigators say Vatican link in “al-Qaeda” arrests. (2015, April 24). *BBC*. Retrieved from http://www.bbc.com/

Jenkins, B. M. (2007). *Building an army of believers—Jihadist radicalization and recruitment* (CT-278-1). Santa Monica, CA: Rand Corporation.

Kadushin, C. (2012). *Understanding social networks: Theories, concepts, and findings*. New York, NY: Oxford University Press.

Kenis, P., & Provan, K. G. (2009). Towards an exogenous theory of public network performance. *Public Administration, 87*(3), 440–456.

Kirkpatrick, D. D. (2014, October 21). New freedoms in Tunisia drive support for ISIS. *The New York Times*. Retrieved from http://www.nytimes.com/

Krauss, C. (2005, November 29). Liberal party loses vote of confidence in Canada. *The New York Times*. Retrieved from http://www.nytimes.com/

Krebs, V. (2001). Mapping networks of terrorist cells. *Connections, 24*(3), 43–52.

Linn, A. (2011, August 23). Post 9/11, surveillance cameras everywhere. *NBC News*. Retrieved from http://www.nbcnews.com/

McChrystal, S. A. (2011). It takes a network: The new front line of modern warfare. *Foreign Policy*, *90*(2), 66–70. Retrieved from http://foreignpolicy.com/

McChrystal, S. A. (2013). *My share of the task: A memoir*. New York, NY: Portfolio/Penguin.

McChrystal, S. A., Collins, T., Silverman, D., & Fussell, C. (2015). *Team of teams: New rules of engagement for a complex world*. New York, NY: Portfolio/Penguin.

McCulloh, I., & Carley, K. M. (2011). Detecting change in longitudinal social networks. *Journal of Social Structure*, *12*(3), 1–37.

Milgram, S. (1967). The small-world problem. *Psychology Today*, *1*(1), 61–67.

Milward, H. B., & Provan, K. G. (2006). *A manager's guide to choosing and using collaborative networks*. Washington, DC: IBM Center for the Business of Government.

Milward, H. B., & Raab, J. (2006). Dark networks as organizational problems: Elements of a theory. *International Public Management Journal*, *9*(3), 333–360.

Morris, N. (2014, October 16). ISIS fighters returning to Britain could face treason trial, says Philip Hammond. *The Independent*. Retrieved from http://www.independent.co.uk/

Mortenson, G., & Relin, D. O. (2006). *Three cups of tea: One man's mission to fight terrorism and build nations—one school at a time*. New York, NY: Viking.

Oliver, K. (2014, June 25). *Covert networks: Structures, processes and types*. Unpublished manuscript, University of Manchester, Manchester, UK.

Osborne, G., & Slay, J. (2011). Digital forensics Infovis: An implementation of a process for visualisation of digital evidence. In *Proceedings of the Sixth International Conference on Availability, Reliability and Security* (pp. 196–201). doi:10.1109/ARES.2011.36

Paris attacks: Suspects' profiles. (2015, January 12). *BBC*. Retrieved from http://www.bbc.com/

Povoledo, E. (2015, April 24). Terrorist cell had sights on Vatican, Italy says. *The New York Times*. Retrieved from http://www.nytimes.com/

Pratkanis, A. R. (2007). *The science of social influence: Advances and future progress*. New York, NY: Psychology Press.

Pratkanis, A. R., & Aronson, E. (1992). *Age of propaganda: The everyday use and abuse of persuasion*. New York, NY: W.H. Freeman.

Prell, C. (2012). *Social network analysis: History, theory & methodology*. Los Angeles, CA: Sage.

Reinares, F., & Elorza, A. (2004). *El nuevo terrorismo islamista: Del 11-S al 11-M*. Madrid, Spain: Temas de Hoy.

Roberts, N. (2003). *Note on organizational system's framework*. Unpublished manuscript, Naval Postgraduate School, Monterey, CA.

Roberts, N. (2013). *Network design continuum: Moving beyond the fault lines in social network theory and research.* Unpublished manuscript, Naval Postgraduate School, Monterey, CA.

Roberts, N., & Everton, S. F. (2011). Strategies for combating dark networks. *Journal of Social Structure, 12*(2), 1–32.

Rodriguez, J. A. (2005). *The March 11 network: In its weakness lies its strength*. Paper presented at the XXV International Sunbelt Social Network Conference, Los Angeles, CA.

Sage, A. (2015, January 9). Charlie Hebdo shooter says financed by Qaeda preacher in Yemen. *Reuters*. Retrieved from http://www.reuters.com/

Sageman, M. (2004). *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.

Silber, M. D., & Bhatt, A. (2007). *Radicalization in the west: The homegrown threat.* New York, NY: New York City Police Department. Retrieved from http://www.nyc.gov/

Swedish Security Service. (2015). *Swedish security service yearbook 2014*. Stockholm, Sweden: Edita. Retrieved from http://www.sakerhetspolisen.se/

Teerlink, S., & Erbacher, R. (2006). Improving the computer forensic analysis process through visualization. *Communications of the ACM, 49*(2), 71–75.

Teotonio, I. (2010). Toronto 18. *Toronto Star*. Retrieved from http://www3.thestar.com/static/toronto18/

Tilly, C. (2005). *Trust and rule*. New York, NY: Cambridge University Press.

The United Nations Statistics Division. (2013). City population by sex, city and city type [Database]. Retrieved August 20, 2015 from http://data.un.org/

U.S. Army. (2011). *ADP 3–0 unified land operations*. Washington, DC: Headquarters, Department of the Army.

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge, United Kingdom; New York, NY: Cambridge University Press.

White, H. C., Boorman, S. A., & Breiger, R. L. (1976). Social structure from multiple networks I: Blockmodels of roles and positions. *American Journal of Sociology*, *81*(4), 730–780.

The World Bank. (2015). GDP growth (annual %) [Table]. Retrieved August 20 from http://data.worldbank.org/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California